(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－287014

(43)公開日　平成８年(1996)11月１日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	9364－5Ｌ	Ｇ０６Ｆ　15/00	３３０Ｚ
Ｇ０９Ｃ　1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６６０Ｅ
		7259－5Ｊ		６６０Ｄ
		7259－5Ｊ		６６０Ｇ
Ｈ０４Ｌ　9/08			Ｈ０４Ｎ　7/15	

審査請求　未請求　請求項の数８　ＯＬ　（全 24 頁）　最終頁に続く

(21)出願番号　特願平7－280984

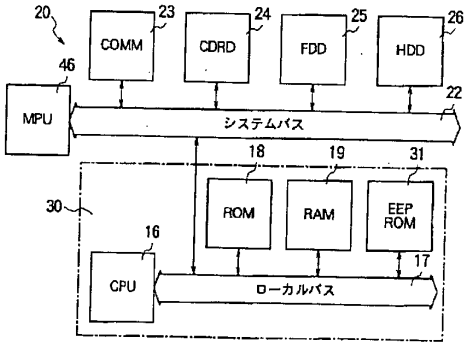
(22)出願日　平成７年(1995)10月27日

(31)優先権主張番号　特願平6－264200
(32)優先日　平６(1994)10月27日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平6－299835
(32)優先日　平６(1994)12月２日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005979
三菱商事株式会社
東京都千代田区丸の内２丁目６番３号
(72)発明者　斉藤　誠
東京都千代田区丸の内二丁目６番３号　三菱商事株式会社内
(72)発明者　籾木　隼一
東京都千代田区丸の内二丁目６番３号　三菱商事株式会社内
(74)代理人　弁理士　南條　眞一郎

(54)【発明の名称】　データ著作権管理装置

(57)【要約】
【課題】　データ著作権・ディジタルキャッシュ及びテレビジョン会議システムデータを取扱う端末装置を提供する。
【解決手段】　ＣＰＵ，ＲＯＭ，ＥＥＰＲＯＭ及びＲＡＭを備え、ＣＰＵのバスにはＲＯＭ，ＥＰＲＯＭ及びＲＡＭが接続されるとともにデータを利用する装置のシステムバスが接続可能とされ、ＲＯＭにはデータ著作権管理システムプログラム、暗号アルゴリズム、ユーザ情報が、ＥＥＰＲＯＭには第２専用鍵、利用許可鍵、第２秘密鍵及び著作権情報が格納され、装置動作時には第１の公開鍵、第１専用鍵、第２公開鍵及び第１秘密鍵がＲＡＭに転送される。データ著作権管理装置の形態としてはモノリシックまたはハイブリッドＩＣ，専用の端子を有する薄型のＩＣカード，ＰＣカード及び挿入用ボードが可能であり、さらにコンピュータ装置、テレビジョン受像器、セットトップボックス、デジタルビデオテープレコーダ、デジタルビデオディスクレコーダ、デジタルオーディオテープ装置あるいは携帯型端末装置等に内蔵させることもできる。



1

【特許請求の範囲】

【請求項１】　ディジタルデータを利用するユーザ端末装置に付属して用いられるデータ著作権管理装置であって、

前記データ著作権管理装置は中央処理装置，中央処理装置バス，読み出し専用半導体メモリ，電気的消去可能プログラマブルメモリ及び読み出し・書き込みメモリを備え、

前記中央処理装置バスには前記中央処理装置，前記読み出し専用半導体メモリ，前記電気電気的消去可能プログラマブルメモリ及び前記読み出し・書き込みメモリが接続されるとともに前記ユーザ端末装置のシステムバスが接続可能とされ、

前記読み出し専用半導体メモリにはデータ著作権管理システムプログラム、暗号アルゴリズム及びユーザ情報が格納され、

前記電気的消去可能プログラマブルメモリには第２の専用鍵，利用許可鍵，第２の秘密鍵，著作権管理プログラム及び著作権情報が格納され、

前記読み出し・書き込みメモリには動作時に第１の公開鍵，第１の専用鍵，第２の公開鍵及び第１の暗号鍵が転送されるデータ著作権管理装置。

【請求項２】　ディジタルデータを利用するユーザ端末装置に付属して用いられるデータ著作権管理装置であって、

前記データ著作権管理装置は中央処理装置，中央処理装置バス，読み出し専用半導体メモリ，電気的消去可能プログラマブルメモリ及び読み出し・書き込みメモリを備え、

前記中央処理装置バスには前記中央処理装置，前記読み出し専用半導体メモリ，前記電気電気的消去可能プログラマブルメモリ及び前記読み出し・書き込みメモリが接続されるとともに前記ユーザ端末装置のシステムバスが接続可能とされ、

前記読み出し専用半導体メモリにはデータ著作権管理システムプログラム，著作権管理プログラム，暗号アルゴリズム及びユーザ情報が格納され、

前記電気的消去可能プログラマブルメモリには第２の専用鍵，利用許可鍵，第２の秘密鍵及び著作権情報が格納され、

前記読み出し・書き込みメモリには動作時に第１の公開鍵，第１の専用鍵，第２の公開鍵及び第１の暗号鍵が転送されるデータ著作権管理装置。

【請求項３】　ＩＣに構成された請求項１または請求項２記載のデータ著作権管理装置。

【請求項４】　ＩＣカードに構成された請求項１または請求項２記載のデータ著作権管理装置。

【請求項５】　ＰＣカードに構成された請求項１または請求項２記載のデータ著作権管理装置。

【請求項６】　挿入ボードに構成された請求項１または

2

請求項２記載のデータ著作権管理装置。

【請求項７】　暗号化されたデジタルデータを復号化処理して表示・加工し、復号化されたデータを再暗号化処理して保存・複写・転送を行うユーザ端末装置で用いるデータ著作権管理装置であって、

前記データ著作権管理装置はマイクロプロセッサ、

前記マイクロプロセッサに接続されるローカルバス、

前記ローカルバスに接続される読み出し専用半導体メモリ及び読み出し・書き込みメモリを備えるコンピュータが構成され、

前記ユーザ端末装置のマイクロプロセッサと前記データ著作権管理装置のマイクロプロセッサのうち一方が復号化処理を行い他方が再暗号化処理を行うデータ著作権管理装置。

【請求項８】　暗号化されたデジタルデータを復号化処理して表示・加工し、復号化されたデータを再暗号化処理して保存・複写・転送を行うユーザ端末装置で用いるデータ著作権管理装置であって、

前記データ著作権管理装置は第１及び第２のマイクロプロセッサを備え、

前記第１のマイクロプロセッサに接続される第１のローカルバス、

前記第１のローカルバスに接続される第１の読み出し専用半導体メモリ及び第１の読み出し・書き込みメモリを備える第１のコンピュータ、

前記第２のマイクロプロセッサに接続される第２のローカルバス、

前記第２のローカルバスに接続される第２の読み出し専用半導体メモリ及び第２の読み出し・書き込みメモリを備える第２のコンピュータが構成され、

前記第１のマイクロプロセッサが暗号化されたデータの復号化処理を行い、

前記第２のマイクロプロセッサが復号化されたデータの再暗号化処理を行うデータ著作権管理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はデジタルデータの表示、保存、複写、加工、転送においてデータを利用する装置に係るものであり、デジタルデータの著作権を保護することを目的とする。

【０００２】

【従来の技術】情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータを通信回線で各々のコンピュータを接続することによって相互に利用するデータベースシステムが普及しつつある。このデータベースシステムにおいてこれまでに扱われてきた情報は古典的なコンピュータで処理することができる情報量が少ないコード化情報及びせいぜいのところでファクシミリ情報のようなモノクローム２値データであり、自然画及び動画のような情報量が格段に多い

データを取扱うことができなかった。

【0003】ところで、各種電気信号のディジタル処理技術が発展する中で、従来はアナログ信号としてのみ扱われていた2値データ以外の画像信号もディジタル処理技術の開発が進められている。この画像信号のディジタル化によりテレビジョン信号のような画像信号をコンピュータで扱うことが可能となるため、コンピュータが扱う各種のデータと画像信号をディジタル化した画像データとを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。

【0004】画像データは、文字データ及び音声データと比較して圧倒的に情報量が多いため、そのままでは保存，転送あるいはコンピュータにおける各種の処理が困難である。そのため、これらの画像データを圧縮／伸張することが考えられ、いくつかの画像データ圧縮／伸張用の規格が作成されてきた。その中で、共通の規格としてこれまでに静止画像用のＪＰＥＧ（Joint Photographic image coding ExpertsGroup ）規格，テレビジョン会議用のＨ．２６１規格，画像蓄積用のＭＰＥＧ１（Moving Picture image coding Experts Group １）規格及び現在のテレビジョン放送から高精細度テレビジョン放送に対応するＭＰＥＧ２規格が作成された。これらの技術により、ディジタル映像データのリアルタイム処理が可能となってきている。

【0005】従来広く普及しているアナログデータは保存，複写，加工，転送をする毎に品質が劣化するために、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、ディジタルデータは保存，複写，加工，転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、ディジタルデータの著作権処理には的確な方法がなく、著作権法であるいは契約で処理されており、著作権法においてもディジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【0006】データベースの利用法は単にその内容を参照するだけでなく、通常は得たデータを保存，複写，加工することによって有効活用し、加工したデータを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオンラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータとして登録することさえ可能である。従来のデータベースシステムにおいては文字データのみが対象となっていたが、マルチメディアシステムにおいては、これまでデータベース化されていた文字等のデータに加えて、本来アナログデータである音声データ及び画像データがディジタル化されてデータベースとされる。

【0007】このような状況において、データベース化されたデータの著作権をどのように取扱うかが大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写，加工，転送等の2次利用について完成された著作権管理手段はない。なお、広告付きソフトあるいはフリーウェア呼ばれるデータは利用において原則として使用料を必要としないが、著作権は存在しており、利用の仕方によっては著作権上の制限を受ける場合がある。本発明者らは特開平６－１４１００４号及び特開平６－１４１００４号で公衆電信電話回線を通じて鍵管理センタから許可鍵を入手することによって著作権管理を行うシステムを、特開平６－１３２９１６号でそのための装置を提案した。

【0008】また、特願平６－６４８８９号及び特願平６－２３７６７３号において、ディジタルデータの著作権を管理するシステムについて提案した。これらのシステム及び装置において、暗号化された番組の視聴を希望する者は通信装置を使用し通信回線を経由して管理センタに視聴申し込みを行い、管理センタはこの視聴申し込みに対して許可鍵を送信するとともに課金処理を行い料金を徴収する。許可鍵を受信した視聴希望者はオンラインあるいはオフライン手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって暗号化された番組の暗号を解除する。

【0009】特願平６－６４８８９号に記載されたシステムは、デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータの表示（音声化を含む），保存，複写，加工，転送における著作権の管理を行うために、利用を許可する鍵の他に、著作権を管理するためのプログラム及び著作権情報を用いる。この著作権管理プログラムは、申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。また、この特願平６－６４８８９号には、データが暗号化された状態でデータベースから供給され、著作権管理プログラムによって表示・加工のときに復号化され、保存，コピー，転送は再び暗号化された状態で行なわれるようにすることが記載されている。さらに、著作権管理プログラム自体を暗号化し、許可鍵で著作権管理プログラムを復号化し、復号化された著作権管理プログラムが著作権データの復号化及び暗号化を行うこと、データの保存及び表示以外の利用が行われた場合には操作者についての情報を含む著作権情報を原著作権情報に加えて履歴として保存することも記載されている。

【0010】初めに暗号技術について一般的な説明をしておく。暗号技術には、秘密鍵暗号方式(secret-key cryptosystem) と、公開鍵暗号方式(public-key cryptosystem) がある。秘密鍵暗号方式は、暗号化と復号化に同じ暗号鍵を使用する暗号方式であり、暗号化及び復号化に要する時間が短い反面、秘密鍵が発見され暗号が解読(Cryptanalize) されてしまうことがある。一方、公開鍵暗号方式は暗号化用の鍵が公開鍵(public-key)として公開されており、復号化用の鍵が公開されていない暗号鍵方式であり、暗号化用の鍵は公開鍵と呼ばれ、復号化

用の鍵は専用鍵(private-key) と呼ばれる。この暗号方式を使用するには、情報を発信する側は暗号を受信する側の公開鍵で暗号化(encrption) し、情報を受信する側は公開されていない専用鍵で復号化(decryption)する暗号方式であり、暗号化及び復号化に要する時間が長い反面、専用鍵を発見することが殆ど不可能であり暗号の解読が非常に困難である。

【００１１】暗号技術においては平文(plaintext) Mを暗号鍵(cryption key)Kを用いて暗号化し暗号文(cryptogram)Cを得る場合を

C＝E（K，M）

と表現し、暗号文Cを暗号鍵Kを用いて復号し平文Mを得る場合を

M＝D（K，C）

と表現する。本発明において使用される暗号方式には、暗号化と復号化に同じ秘密鍵Ｋｓ が使用される秘密鍵方式(secret-key system) と、平文の暗号化に公開鍵(publickey)Ｋｂ が使用され、暗号文の復号化に専用鍵(private-key)Ｋｖ が使用される公開鍵方式(public-key system) が採用される。

【００１２】図１に示されたのは、本願発明に係るデータ著作権管理装置が使用される先願である特願平６－２３７６７３号に示されたデータ著作権管理システムの構成である。このシステムでは、暗号化データが１次ユーザ４からの要求に応じて双方向的に供給される。また、暗号鍵方式として秘密鍵方式及び公開鍵方式が採用される。なお、このシステムがデータ供給手段としてデータベース以外に広告付き等の無料の暗号化する必要の無い衛星放送，地上波放送，ＣＡＴＶ放送あるいは記録媒体を用いる場合にも適用可能なことは勿論のことである。

【００１３】このシステムにおいて、１はデータベース、４は１次ユーザ端末装置、５は２次ユーザ端末装置、６は３次ユーザ端末装置、７はｎ次ユーザ端末装置である。また、３は著作権管理センタ、８，９及び１０は著作権管理センタ３に保管されている２次著作権データ，３次著作権データ・・・ｎ次著作権データ、２は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡＴＶ回線等の通信ネットワークである。

【００１４】これらのうち、データベース１、１次ユーザ端末装置４、２次ユーザ端末装置５、３次ユーザ端末装置６、ｎ次ユーザ端末装置７、著作権管理センタ３は通信ネットワーク２に接続されており相互に接続可能である。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、１点鎖線で示された経路は各データからの利用形態に対応した許可情報とともに暗号鍵が転送される経路であり、２点鎖線で示された経路はデータベースからあるいは著作権管理センタ内でデータから次位のデータへ著作権情報が転送される経路である。また、このシステムを利用する各ユーザは予めデータベース組織に登録をしておく。また、この登録の際にデータベース組織利用ソフトウェアがユーザに対して提供される。このデータベース組織利用ソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に暗号化された著作権管理データをこれを復号化するためのプログラムが含まれている。

【００１５】データベース１を利用するに当たり、１次ユーザは１次ユーザ認証データＡｕ1，第１公開鍵Ｋｂ1及び第１公開鍵Ｋｂ1に対応する第１専用鍵Ｋｖ1，第２公開鍵Ｋｂ2及び第２公開鍵Ｋｂ2に対応する第２専用鍵Ｋｖ2を用意し、１次ユーザ端末装置４を利用し通信ネットワーク２を経由してデータベース１にアクセスする。

【００１６】１次ユーザから１次ユーザ認証データＡｕ1，第１公開鍵Ｋｂ1、第２公開鍵Ｋｂ2の転送を受けたデータベース１は、１次ユーザ認証データＡｕ1を確認し、確認された１次ユーザ認証データＡｕ1を１次ユーザ情報Ｉｕ1として２次著作権管理センタ３に転送する。

【００１７】一方、データベース１は２個の秘密鍵すなわち第１の秘密鍵Ｋｓ1と第２の秘密鍵Ｋｓ2を用意する。用意された第１の秘密鍵Ｋｓ1及び第２の秘密鍵Ｋｓ2中、第２の秘密鍵Ｋｓ2も予め著作権管理センタ３に転送される。

【００１８】これらの転送が行われた結果著作権管理センタ３には１次利用形態に対応する許可鍵Ｋｐ、１次ユーザ情報Ｉｕ1、原著作権情報Ｉｃ0及び第２秘密鍵Ｋｓ2が格納される。なお、これらの中で原著作権情報Ｉｃ0は著作権使用料金分配に用いられる。

【００１９】データの利用を希望する１次ユーザは、１次ユーザ端末装置４を利用してデータベース１にアクセスすると、データメニューが転送される。このときデータメニューとともに料金の情報を表示してもよい。

【００２０】データメニューが転送されると１次ユーザはデータメニュー検索を行いデータMを選択する。このとき、選択されたデータMの原著作権情報Ｉｃ0が著作権管理センタ３に転送される。また、１次ユーザは視聴・保存・複写・加工・転送である利用形態に対応した許可鍵の中から希望する利用形態に対応した許可鍵Ｋｐ1を選択する。この許可鍵Ｋｐ1も著作権管理センタ３に転送される。

【００２１】なお、１次ユーザが行う利用形態として視聴・保存は最低限必要であるから、これらの利用形態は最小限の利用形態として選択の対象から外し、複写・加工・転送のみを選択の対象とすることもできる。

【００２２】１次ユーザの要求に応じてデータベース１から原データM0 が読み出される。読み出された原データM0 は第１秘密鍵Ｋｓ1で暗号化される。

Cm0ks1=E（Ks1，M0）

この暗号化データＣm0ks1 には暗号化されていない原著作権者情報Ｉｃ0が付けられている。また、第１の秘密鍵

Ks1を第1の公開鍵Kb1で、第2の秘密鍵Ks2を同じく第2の公開鍵Kb2で暗号化する。

Cks1kb1= E（Kb1, Ks1）

Cks2kb2= E（Kb2, Ks2）

併せて著作権管理プログラムPも第2の秘密鍵Ks2で暗号化されるが、

Cpks2= E（Ks2, P）

著作権管理プログラムPの暗号化は第2の秘密鍵Ks2で暗号化されなければならないものではなく、他の適当な暗号鍵を用いて暗号化することができる。暗号化原データCm0ks1 、暗号化著作権管理プログラムCpks2及び2個の暗号化秘密鍵Cks1kb1, Cks2kb2が通信ネットワーク2を経由して1次ユーザ端末装置4に転送される。このときに必要ならば課金が行われる。なお、暗号化著作権管理プログラムCpks2はデータベース1から供給されるのではなく、ユーザ端末装置4内の例えばROMに内蔵しておくことも可能である。

【0023】データベース1から暗号化原データCm0ks1，2個の暗号化秘密鍵Cks1kb1,Cks2kb2及び暗号化著作権管理プログラムCpks2を受け取った1次ユーザは、データベース組織利用ソフトウェアを利用して第1公開鍵Kb1に対応する第1専用鍵Kv1を用いて暗号化第1秘密鍵Cks1kb1を復号化し、

Ks1= D（Kv1, Cks1kb1）

第2公開鍵Kb2に対応する第2専用鍵Kv2を用いて暗号化第2秘密鍵Cks2kb2を復号化する。

Ks2= D（Kv2, Cks2kb2）

さらに、復号化された第2秘密鍵Ks2を用いて暗号化著作権管理プログラムCpks2を復号化する。

P= D（Ks2, Cpks2）

【0024】最後に、復号化された著作権管理プログラムPを利用して復号化された第1秘密鍵Ks1を用いて暗号化データCm0ks1 を復号化し、

M0=D（Ks1, Cm0ks1）

復号化された原データM0 をそのままあるいは加工データM1 として利用する。前に説明したように、第1専用鍵Kv1及び第2専用鍵Kv2は1次ユーザが用意し他には公開していない暗号鍵であるから、第3者がデータMを入手したとしても暗号化データMを復号化して利用することは不可能である。

【0025】以後原データM0 あるいは加工データM1 であるデータMの保存、コピーあるいは転送を行う場合には第2秘密鍵Ks2を用いて暗号化及び復号が行われる。

Cmks2= E（Ks2, M）

M= D（Ks2, Cmks2）

復号された第2の秘密鍵Ks2は以後データの保存、コピーあるいは転送を行う場合にデータの暗号化／復号化を行う際の暗号鍵として用いられる。1次ユーザ端末装置4には、これらの第1専用鍵Kv1及び第2専用鍵Kv2、第1の秘密鍵Ks1及び第2秘密鍵Ks2，データM，著作権管理プログラムPとともに原著作権情報Ic0及び1次ユーザがデータの加工を行った場合には1次ユーザ情報及び加工日時等である著作権情報Ic1も格納される。なお、この著作権情報Ic1は著作権情報ラベルとしてデータに付けるようにし、さらにディジタル署名付にしておけば安全である。暗号化データCmks2は暗号化されて流通し、復号鍵である第2秘密鍵Ks2を入手するためには、著作権情報ラベルが手がかりとなるから、暗号化データCmks2からこの著作権情報ラベルが取り外された場合には、第2秘密鍵Ks2を入手することができない。

【0026】暗号化データCmks2が1次ユーザ端末装置4内に保存された場合には第2の秘密鍵Ks2が装置内に保存されるが、暗号化データCmks2が1次ユーザ端末装置4内に保存されることなく記憶媒体11にコピーあるいは通信ネットワーク2を経由して2次ユーザ端末装置5への転送が行なわれた場合には、1次ユーザ端末装置4における以降の利用を不可能にするために第2の秘密鍵Ks2が廃棄される。なお、この場合コピー・転送回数に制限を設けて、制限回数内のコピー・転送では第2の秘密鍵Ks2が廃棄されないようにしてもよい。

【0027】データMを外部記憶媒体11にコピーあるいは通信ネットワーク2を経由して転送しようとする1次ユーザは、コピーあるいは転送を行うにあたって第2秘密鍵Ks2を用意し、データMを第2の秘密鍵Ks2を用いて暗号化する。

Cmks2= E（Ks2, M）

この暗号化データCmks2には暗号化されていない原著作権情報Ic0、1次ユーザの著作権情報Ic1が付加される。

【0028】2次ユーザは、データベース使用前に1次ユーザと同様に2次ユーザを認証するための認証データAu2，第3の公開鍵Kb3及び第3の公開鍵Kb3に対応する第3の専用鍵Kv3，第4の公開鍵Kb4及び第4の公開鍵Kb4に対応する第4の専用鍵Kv4を用意する。

【0029】コピーあるいは転送された暗号化データCmks2の2次利用を希望する2次ユーザは、2次ユーザ端末装置5を利用して通信ネットワーク2を経由して著作権管理センタ3に対してデータ名あるいはデータ番号を指定して2次利用申込を行うが、そのときに、2次ユーザ認証データAu2、原著作権情報Ic0及び1次ユーザ著作権情報Ic1に加えて第3の公開鍵Kb3と第4の公開鍵Kb4も転送する。

【0030】2次ユーザからの2次利用申込を受けた著作権管理センタ3は、2次ユーザの認証データAu2を確認し、確認された2次ユーザ認証データAu2は2次ユーザ情報として3次著作権データ9に転送される。また、1次ユーザの2次著作権情報Ic1が転送された場合には2次著作権情報Ic1を2次著作権データ8に照会・確認し、確認された2次的著作権情報Ic1は3次著作権デー

タ9に転送される。

【0031】2次ユーザは視聴・蓄積・複写・加工・転送の利用形態に対応した許可鍵Kp2を選択する。選択された利用形態に対応した許可鍵Kp2は3次著作権データベース9に転送される。なお、2次ユーザの利用形態として視聴・蓄積は最低限必要であるから、これらの利用形態は最小限の利用形態として選択の対象から外し、複写・加工・転送のみを選択の対象としてもよい。

【0032】2次著作権データベース8は、第3の秘密鍵Ks3を用意する。用意された第3の秘密鍵Ks3は3次著作権データ9に転送され格納される。

【0033】これらの転送が行われた結果、3次著作権データ9には許可鍵Kp2、1次ユーザ著作権情報Ic1、1次ユーザ情報Iu1、原著作権情報Ic0、2次ユーザ情報Iu2及び第3の秘密鍵Ks3が格納される。これらの中、許可鍵Kp2と1次ユーザ著作権情報Ic1及び1次ユーザ情報Iu1は、著作権使用料金分配に用いられる。

【0034】以下同様にして、n次著作権データ10にはn次利用形態に対応した許可鍵Kpn、（n－1）次ユーザの2次的著作権情報Icn-1、1次ユーザ情報Iu1、原著作権情報Ic0、n次ユーザ情報Iun及び第nの秘密鍵Ksnが格納される。

【0035】2次著作権データ8から許可鍵Kp2、1次ユーザ情報Iu1、原著作権情報Ic0及び第2の秘密鍵Ks2が読み出される。この中、原著作権情報Ic0は著作権使用料配分のために使用される。読み出された第2の秘密鍵Ks2は2次ユーザの第3の公開鍵Kb3を用いて、第3の秘密鍵Ks3は同じく第4の公開鍵Kb4を用いて暗号化される。

$Cks2kb3 = E(Kb3, Ks2)$

$Cks3kb4 = E(Kb4, Ks3)$

また、著作権管理プログラムPは第3の秘密鍵Ks3を用いて暗号化される。

$Cpks3 = E(Ks3, P)$

暗号化著作権管理プログラムCpks3及び暗号化第2秘密鍵Cks2kb3及び暗号化第3秘密鍵Cks3kb4が通信ネットワーク2を経由して2次ユーザ端末装置5に転送される。このときに必要ならば課金が行われる。

【0036】2次著作権データ8から暗号化された2個の秘密鍵Cks2kb3及びCks3kb4及び暗号化された著作権管理プログラムCpks3を受け取った2次ユーザは、データベース利用ソフトウェアを利用して第3専用鍵Kv3を用いて暗号化第2秘密鍵Cks2kb3を復号し、第4の公開鍵Kb4に対応する第4の専用鍵Kv4を用いて暗号化第3秘密鍵Cks3 Kb4を復号する。

$Ks2 = D(Kv3, Cks2kb3)$

$Ks3 = D(Kv4, Cks3kb4)$

また、復号化された第3の秘密鍵Ks3を用いて暗号化著作権管理プログラムCpks3が復号される。

$P = D(Ks3, Cpks3)$

次に、復号化された著作権管理プログラムPを利用して復号された第2の秘密鍵Ks2を用いて暗号化データCmks2を復号化し利用する。

$M = D(Ks2, Cmks2)$

【0037】前に説明したように、第3専用鍵Kv3及び第4専用鍵Kv4は2次ユーザが用意したものは他には公開していない暗号鍵であるから、第3者が暗号化データCmks2を入手したとしても復号化して利用することは不可能である。

【0038】このシステムを利用する各ユーザは予めデータベース組織に登録をしておく必要があり、また、この登録の際にデータベース用ソフトウェアがユーザに対して提供される。このソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に第1暗号鍵を用い著作権管理プログラムを復号するためのプログラムが含まれているため、その保護を図る必要がある。また、データMを利用するために第1暗号鍵K1、第2暗号鍵K2及び著作権管理プログラムPが各ユーザに対して転送され、各ユーザはこれらを保管しておく必要がある。さらには著作権情報ラベル、ユーザ情報、公開鍵方式の公開鍵と専用鍵そして秘密鍵生成アルゴリズムを含むプログラム等が必要に応じて保管される。

【0039】これらを保管しておく手段としてフレキシブルディスクを使用することが最も簡便な手段であるが、フレキシブルディスクはデータの消失あるいは改竄に対して極めて脆弱である。また、ハードディスクドライブを使用した場合にもフレキシブルディスク程ではないがデータの消失あるいは改竄に対する不安がある。ところで、最近カード形状の容器にIC素子を封入したICカードが普及し、特にマイクロプロセッサを封入したPCカードがPCMCIAカードあるいはJEIDAカードとして規格化が進められている。

【0040】先願である特願平6－237673号で本発明者らが提案したデータ著作権管理装置を図2により説明する。このデータ著作権管理装置15は、マイクロプロセッサ（CPU）16、CPU16のローカルバス17、ローカルバス17に接続された読み出し専用メモリ（ROM）18及び書き込み・読み出しメモリ（RAM）19を有するコンピュータシステムとして構成されており、ローカルバス17がユーザ端末装置20のマイクロプロセッサ21のシステムバス22に接続される。

【0041】また、ユーザ端末装置20のシステムバス22には装置外部のデータベースからデータを受け取り、データを外部へ転送する通信装置（COMM）23、CD－ROMで供給されるデータを読み込むCD－ROMドライブ（CDRD）24、受け取ったデータあるいは加工したデータを外部へ供給するためにフレキシブルディスクドライブに複写するフレキシブルディスクドライブ（FDD）25及びデータを保存するハードディスクドライブ（HDD）26が接続される。なお、ユ

ーザ端末装置のシステムバス２２には当然のこととしてROM、RAM等が接続されているが、この図においては記載が省略されている。

【００４２】データ著作権管理装置１５のROM１８には、データベースを利用するためのソフトウェア及びユーザデータ等の固定した情報が格納されている。RAM１９には鍵管理センタあるいは著作権管理センタから供給された暗号鍵及び著作権管理プログラムが格納される。復号化あるいは再暗号化の作業はデータ著作権管理装置１５が行い、処理結果だけがローカルバス１７及びユーザ端末装置のシステムバス２１を経由してユーザ端末装置２０に転送される。このデータ著作権管理装置１５は、モノリシックＩＣ、ハイブリッドＩＣ、拡張ボード、ＩＣカードあるいはＰＣカードとして実現される。

【００４３】

【発明の概要】本件出願においては、先願である特願平６－２３７６７３号で提案されたユーザ端末装置に付属して用いるデータ著作権管理装置をさらに具体的にしたデータ著作権管理装置を提案する。本発明のデータ著作権管理装置は、ユーザ端末装置に付属して用いられ、中央処理装置，中央処理装置バス，読み出し専用半導体メモリ，電気的消去可能プログラマブルメモリ及び読み出し・書き込みメモリを備えている。中央処理装置バスには中央処理装置，読み出し専用半導体メモリ，電気的消去可能プログラマブルメモリ及び読み出し・書き込みメモリが接続されるとともにデータを利用する装置のシステムバスが接続可能とされ、読み出し専用半導体メモリにはデータ著作権管理システムプログラム、暗号アルゴリズム及びユーザ情報が格納され、電気的消去可能プログラマブルメモリには第２の専用鍵、利用許可鍵、第２の秘密鍵及び著作権情報が格納され、装置動作時には読み出し・書き込みメモリに第１の公開鍵、第１の専用鍵、第２の公開鍵及び第１の秘密鍵が転送される。著作権管理プログラムは外部から供給される場合にはＥＥＰＲＯＭに格納されるが、そうでない場合にはＲＯＭに格納される。データ著作権管理装置の形態としてはモノリシックＩＣ，ハイブリッドＩＣ，専用の端子を有する薄型のＩＣカード，ＰＣカード及び挿入用ボードが可能である。

【００４４】これまでに先願発明として説明したデータ著作権管理システムにおいては、入手した暗号化データを表示・加工する場合には復号化して利用するが、入手あるいは加工したデータを保存・複写・転送する場合には再暗号化することによって、データの不正規な使用ができないようにしている。したがって、本発明が対象とするデータ著作権管理システムで使用される装置においては、データの復号化だけでなく、データの再暗号化も同時に行われる必要があるが、これらの先願に記載されたデータ著作権管理装置はデータの復号化あるいは再暗号化の作業のうち一方のみしか実行することができない。

【００４５】そこで、本願においては著作権を管理するために暗号化されて供給されるデータを復号化と再暗号化を同時に行うことができるデータ著作権管理装置の発明を提案する。そのために、ユーザ端末装置においてユーザ端末装置全体を制御するマイクロプロセッサに加えて少なくとも１個のマイクロプロセッサ、理想的には２個のマイクロプロセッサ、を付加させることにより暗号化されて供給されたデータの復号化及び再暗号化を行う。１個のマイクロプロセッサが付加される場合は、ユーザ端末装置のマイクロプロセッサと付加されたマイクロプロセッサの中一方がデータの復号化を行い、他方が再暗号化を行う。２個のマイクロプロセッサが付加される場合は、付加されたマイクロプロセッサの中の一方がデータの復号化を行い、他方のマイクロプロセッサが再暗号化を行い、ユーザ端末装置２０のマイクロプロセッサは全体の動作を制御する。

【００４６】付加されるマイクロプロセッサはユーザ端末装置のマイクロプロセッサのシステムバスに接続してもよいが、この構成ではマイクロプロセッサを並行して動作させるマルチプロセッサ構成を実現することはできない。そこで、本願においてはＳＣＳＩバスあるいはＰＣＩバスを利用してマルチプロセッサ構成としたデータ著作権管理装置を提案する。

【００４７】デジタルデータには、文字データの他にグラフィックデータ、コンピュータプログラム、デジタル音声データ、ＪＰＥＧ等の方式による静止画データ、さらにはＭＰＥＧ等による動画データがある。これらのデータからなるデータ著作物は種々の装置を用いて利用されるが、これらの装置にもデータ著作権管理機能を具えておく必要がある。そこで、本出願においてはこれらのデータ著作権管理装置及び先願に記載されたデータ著作権管理装置の使用形態として種々の装置に内蔵することを提案する。

【００４８】

【実施例】以下、本願発明の実施例を図面を用いて説明する。図３に示されたのは、実施例１である本願発明に係るデータ著作権管理装置の構成を示すブロック図である。このデータ著作権管理装置３０は、先願である特願平６－２３７６７３号に記載されたデータ著作権管理装置１５の構成要素に加えて電気的消去可能プログラマブルメモリ（ＥＥＰＲＯＭ）３１を備えている。このデータ著作権管理装置３０は、ＣＰＵ１６、ＣＰＵ１６のローカルバス１７、ローカルバス１７に接続されたＲＯＭ１８、ＲＡＭ１９及びＥＥＰＲＯＭ３１を有するコンピュータシステムであり、ローカルバス１７がユーザ端末装置２０のマイクロプロセッサ２１のシステムバス２２に接続される。また、ユーザ端末装置２０のシステムバス２２には装置外部のデータベースからデータを受け取り、データを外部へ転送する通信装置（ＣＯＭＭ）２

3、CD－ROMで供給されるデータを読み込むCD－ROMドライブ（CDRD）24、受け取ったデータあるいは加工したデータを外部へ供給するためにフレキシブルディスクドライブに複写するフレキシブルディスクドライブ（FDD）25及びデータを保存するハードディスクドライブ（HDD）26が接続される。なお、ユーザ端末装置のシステムバス22には当然のこととしてROM、RAM等が接続されているが、この図においては記載が省略されている。

【0049】ROM18には、データ著作権管理プログラム、暗号アルゴリズムに基づく暗号プログラム及びユーザデータ等の固定した情報が格納されている。EEPROM31には暗号鍵及び著作権情報が格納される。なお、データ著作権管理プログラム及び暗号プログラムがデータベース等外部から供給される場合には、これらはROM18ではなく、EEPROM31に格納される。復号化あるいは再暗号化の作業はデータ著作権管理装置30が行い、処理結果だけがローカルバス17及びシステムバス22を経由してユーザ端末装置20に転送される。

【0050】このデータ著作権管理装置30は、モノリシックIC、ハイブリッドIC、拡張ボード、ICカードあるいはPCカードとして実現される。

【0051】実施例1のデータ著作権管理装置30のROM18には、データ著作権管理プログラム、暗号アルゴリズムに基づく暗号プログラム及びユーザデータ等の固定した情報が格納されている。なお、このROM18には秘密ではない秘密鍵アルゴリズムに基づく秘密鍵生成プログラム、復号化プログラム及び再暗号化プログラムを格納することができる。EEPROM31には暗号鍵及び著作権情報が格納される。なお、著作権管理プログラム及び暗号プログラムがデータベース等外部から供給される場合には、これらはROM18ではなく、EEPROM31に格納される。なお、このEEPROMは必ずしも必要なものではなく、省略することも可能である。RAM19には鍵管理センタあるいは著作権管理センタから供給される第1暗号鍵あるいは第2暗号鍵の一方及びデータ著作権管理システムプログラムが格納される。

【0052】一方、ユーザ端末装置20のMPU46が必要とするソフトウェア及びユーザデータ等の情報はソフトウェアによりユーザ端末装置20に供給され、ユーザ端末装置20のRAMに格納されている。また、ユーザ端末装置20のRAMには鍵管理センタあるいは著作権管理センタから供給される第1暗号鍵あるいは第2暗号鍵の一方及び著作権管理システムプログラムが格納される。復号化及び再暗号化の作業はユーザ端末装置20本体のMPU46とデータ著作権管理装置30のCPU16が分担して、一方が復号化を他方が再暗号化を行い、データ著作管理装置30の処理結果だけがユーザ端末装置に転送される。

【0053】図4により、図3に示されたデータ著作権管理装置30の具体的な内部構成を示す。データ著作権管理装置30には、マイクロコンピュータ（CPU）16、読み出し専用メモリ（ROM）18、書き込み・読み出しメモリ（RAM）19及び電気的消去可能プログラマブルメモリ（EEPROM）31が封入され、これらがマイクロコンピュータ16のマイクロコンピュータバス17に接続されており、さらにこのマイクロコンピュータバス17はユーザ端末装置20本体のシステムバス22に接続されている。

【0054】読み出し専用半導体メモリ18にはデータ著作権管理システムプログラム，暗号アルゴリズム及びユーザ情報が格納されている。電気的消去可能プログラマブルメモリ31の内部は3つのエリアに区分される。第1エリア35には第1公開鍵Kb1，第1専用鍵Kv1，第2公開鍵Kb2及び第2専用鍵Kv2が格納される。第2エリア36には著作権管理プログラムP，視聴許可・蓄積許可・複写許可・加工許可・転送許可等の1次利用における許可鍵となる第1秘密鍵Ks1及び視聴許可・蓄積許可・複写許可・加工許可・転送許可等の2次利用における許可鍵となる第2秘密鍵Ks2が格納される。なお、著作権管理プログラムが外部から供給されるのではなく、ユーザ側に予め置かれることがあるが、その場合著作権管理プログラムは電気的消去可能プログラマブルメモリ31の第2のエリア36ではなく、読み出し専用メモリ18に格納される。第3エリア37には原著作権情報、2次著作権情報等の著作権情報及びアクセスコントロールキーが格納される。

【0055】電気的消去可能プログラマブルメモリ31と同様に、書き込み・読み出しメモリ19の内部も3つのエリアに区分される。第1エリア32には動作時に第1公開鍵Kb1，第1専用鍵Kv1及び第2公開鍵Kb2が格納される。第2エリア33には動作時に視聴許可・蓄積許可・複写許可・加工許可・転送許可等の1次利用における許可鍵となる第1秘密鍵Ks1が格納される。第3エリア34には動作時にアクセスコントロールキーが格納される。

【0056】このデータ著作権管理装置を付属させたユーザ端末装置はデータを利用するためのすべての作業を本発明に係るデータ著作権管理装置内で行い、結果だけをユーザ端末装置に転送し各種の利用を行うようにするので、安全性が高い。

【0057】情報量が多い画像データを送・受信する場合には、通信データ量を減少させるために原データを圧縮してから送信し、被圧縮データを受信後に伸張して利用するが、この場合にもデータを暗号化することにより著作権管理を行うことが可能である。図5に示されたのは、暗号化されるデータがJPEG規格あるいはMPEG規格で圧縮されたデジタル画像である場合のデータ著

作権管理フローの例であり、このフローは伝送線路を挟んで送信側フローと受信側フローに分けられ、さらに受信側フローは表示フローと保存フローに分けられる。

【００５８】送信側における信号処理はデジタル画像を用意する過程と用意されたデジタル画像を処理する過程から構成されている。この過程において原画像がデジタル画像４１である場合にはそのまま次の処理が行われるが、原画像がアナログ画像４０である場合にはデジタル化処理４２が行われる。デジタル画像は初めにＪＰＥＧ規格、ＭＰＥＧ規格等の所定の規格により圧縮処理４３され、圧縮されたデジタルデータは第１秘密鍵を用いて暗号化４４される。

【００５９】このような送信側信号処理が行われた画像データは、衛星放送電波、地上波放送電波、ＣＡＴＶ電波あるいは公衆回線・ＩＳＤＮ回線等の伝送線路４５を経由して伝送される。なお、この伝送線路としてデジタルビデオテープ、デジタルビデオディスクあるいはＣＤ－ＲＯＭ等の記録媒体を使用する場合もある。

【００６０】このようにして受信側に伝送された画像データは初めに第１秘密鍵を用いて復号化４６され、次に圧縮された画像データの伸張４７が行われ、表示４９される。表示装置がデジタルデータ表示装置である場合にはそのまま表示されるが、アナログデータ表示装置である場合にはアナログ化４８が行われる。

【００６１】データがハードディスク、フレキシブルディスク、光磁気ディスク、追記型ビデオディスク等に保存される場合には第２秘密鍵を用いて再暗号化５０された上で、保存される。再暗号化されて保存された画像データを再度表示する場合には、第２秘密鍵を用いて再復号化５２され、表示４９される。表示装置がデジタルデータ表示装置である場合にはそのまま表示されるが、アナログデータ表示装置である場合にはアナログ化４８が行われる。なお、データが画像以外のデータである場合のデータ圧縮／伸張手段及び伝送経路はそのデータに適合した適宜なものが使用される。

【００６２】図６に示されたのは、先願である特願平６－２３７６７３号に示されたデータベース著作権管理システムの例であり、このシステムにおいては暗号鍵方式として秘密鍵方式が採用される。この図に示すシステムにおいて、１はテキストデータ，コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ，ディジタル音声データ，ディジタル映像データが暗号化された状態で格納されたデータベースであり、１４は通信・放送衛星等の人工衛星、１５’はＣＤ－ＲＯＭあるいはフレキシブルディスク等のデータ記録媒体、２は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡＴＶ回線等の通信ネットワーク、４は１次ユーザ端末装置である。また、１６は秘密鍵を管理する鍵管理センタ、１７はデータベース著作権を管理する著作権管理センタである。

【００６３】５，６及び７は各々２次ユーザ端末装置，３次ユーザ端末装置及びｎ次ユーザ端末装置であり、１１，１２及び１３は各々フレキシブルディスクあるいはＣＤ－ＲＯＭ等の記憶媒体である２次ディスク，３次ディスク及びｎ次ディスクである。なお、このｎは任意の整数でありｎが４よりも大きい場合には３次ユーザ端末装置６とｎ次ユーザ端末装置７の間及び３次ディスク１２とｎ次ディスク１３との間には対応するユーザ端末装置及びディスクが配置されている。

【００６４】これらのうちデータベース１、鍵管理センタ１６、著作権管理センタ１７、１次ユーザ端末装置４、２次ユーザ端末装置５、３次ユーザ端末装置６及びｎ次ユーザ端末装置７は通信ネットワーク２に接続されている。この図において、破線で示された経路は暗号化されたデータの経路であり、実線で示された経路は各ユーザ端末装置からの要求の経路であり、１点鎖線で示された経路は各データベースからの利用形態に対応した許可情報とともに秘密鍵が転送される経路である。また、このシステムを利用する各ユーザは予めデータベース組織に登録をしておく。また、この登録の際にデータベース組織利用ソフトウェアがユーザに対して提供される。このデータベース組織利用ソフトウェアにはデータ通信用プロトコル等の通常の通信用ソフトウェアの他に著作権管理プログラムを動作させるためのプログラムが含まれている。

【００６５】データベース１あるいはデータ記録媒体１５’に格納されているテキストデータ，コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ，ディジタル音声データ，ディジタル映像データである原データＭ０が通信ネットワーク２、人工衛星１４あるいは記憶媒体１５’を経由して１次ユーザ端末装置４に一方向的に供給されるが、このときには第１秘密鍵Ｋｓ１を用いて暗号化される。

$$C_{m0ks1}=E(K_{s1}, M0)$$

なお、広告付等の無料で提供されるデータの場合でも著作権保護のためには、暗号化を必要とする。

【００６６】先願である特願平６－６４８８９号には、データの利用形態には、最も基本的な表示の他に保存、加工、コピー、転送があり、利用許可鍵はこれらの利用形態のうちの１つあるいは複数に対応するものが用意され、その管理は著作権管理プログラムによって実行されることが示されている。また、データの表示及び加工のための表示以外の利用形態すなわちデータが保存、コピー、転送される場合には著作権管理プログラムによりデータが再暗号化されることが述べられている。いいかえれば、著作権が主張されたデータは暗号化された状態で流通し、平文化されるのは著作権処理機能を有するユーザ端末装置において、表示あるいは加工のための表示が行われるときのみである。

【００６７】このシステムでは、これら先願に記載され

た事項を利用する。供給された暗号化データCm0ks1 の1次利用を希望する1次ユーザは鍵管理センタ16に対して1次ユーザ端末装置4を利用し通信ネットワーク2を経由して原データ名あるいは原データ番号等を指定することにより暗号化原データCm0ks1 の1次利用申込を行うが、このときに1次ユーザに関する情報Iu1を鍵管理センタ16に提示する。1次ユーザ端末装置4を利用しての1次利用申込を受けた鍵管理センタ16は、著作権管理プログラムPとともに1次ユーザがデータベース1から入手した暗号化原データCm0ks1 を復号化するための第1秘密鍵Ks1及び復号された原データM0 あるいは原データを加工して得られた加工データM1 を再暗号化するための第2秘密鍵Ks2を通信ネットワーク2を経由し1次ユーザ端末装置4に転送する。

【0068】復号鍵である第1秘密鍵Ks1、暗号化／復号化鍵である第2秘密鍵Ks2を受け取った1次ユーザ端末装置4において、初めに著作権管理プログラムPを利用して第1秘密鍵Ks1を用いて暗号化原データCm0ks1 を復号化し

M0=D（Ks1, Cm0ks1）

復号化された原データM0 をそのままあるいは加工データM1 として利用する。

【0069】原データM0 あるいは加工データM1 であるデータMが1次ユーザ端末装置4の内部、すなわちメモリあるいは内蔵のハードディスクドライブに保存されている状態ではそのデータを利用することができるのは1次ユーザのみであるが、データMがフレキシブルディスク等の外部記憶媒体11にコピーされた場合、あるいは通信ネットワーク2を経て2次ユーザ端末装置5に転送された場合には、2次利用による著作権の問題が生じる。

【0070】また、1次ユーザが入手した原データM0 をそのまま複写して2次ユーザに供給した場合にはその原データM0 に何等の改変も加えられていないため、そのデータM0 に1次ユーザの著作権は発生しない。しかし、1次ユーザが入手したデータM0 を基に加工を行った場合あるいは他のデータと組み合わせる等の手段を用いることにより新しいデータM1 を作成した場合にはそのデータM1 に1次ユーザの著作権（2次的著作権 secondary exploitation right）が発生する。同様に、2次ユーザが1次ユーザから入手した原データM0 あるいは加工データM1 を基に加工を行った場合あるいは他のデータと組み合わせる等の手段を用いることにより新しいデータM2 を作成した場合には、同様に2次ユーザの著作権が発生する。

【0071】この著作権の問題に対処するため、このシステムにおいてはデータMの保存、コピー、転送が行われるときには著作権管理プログラムPにより第2秘密鍵Ks2を用いてデータMが暗号化され、以後1次ユーザ端末装置4においては第2秘密鍵Ks2を用いてデータMの復号化及び暗号化が行われる。

Cmks2= E（Ks2, M）

M= D（Ks2, Cmks2）

なお、1次ユーザがデータの表示及び加工を行い加工データを得ることは原則として自由にできるが、その場合は著作権管理プログラムにとってその回数に制限を設けることができる。

【0072】外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク8を経てデータが転送されたときには1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は著作権管理プログラムPによって廃棄される。したがって、1次ユーザが再度データMを利用する場合には鍵管理センタ16に利用申込を行い、第2秘密鍵Ks2の再交付を受ける必要がある。この第2秘密鍵Ks2の再交付を受けたことは、データMが外部記憶媒体11へコピーあるいは通信ネットワーク2を経由しての2次ユーザ端末装置5へ転送されることによる2次利用が行われたことを意味するから、このことが鍵管理センタ16から著作権管理センタ17に登録され、以後の2次利用が可能になる。

【0073】1次ユーザ端末装置4からの2次ユーザ端末装置5へのデータMの移動は外部記憶媒体11によってあるいは通信ネットワーク2により行われ、外部記憶媒体11へのコピーあるいは通信ネットワーク2を経由して移動が行われるときには、第2秘密鍵Ks2を用いてデータMが暗号化される。

【0074】外部記憶媒体11にデータMがコピーされたとき及び通信ネットワーク2を経てデータMが転送されたときに1次ユーザ端末装置4内の第1秘密鍵Ks1及び第2秘密鍵Ks2は廃棄されるが、このときに1次ユーザ端末装置4内に保存されている暗号化データCmks2に、暗号化されていない1次ユーザ情報Iu1が付加され、暗号化データCmks2を2次ユーザに転送する際に1次ユーザ情報Iu1も転送される。

【0075】1次ユーザからコピーあるいは転送された暗号化データCmks2の2次利用を希望する2次ユーザは、2次ユーザ端末装置5を利用して通信ネットワーク2を経由して著作権管理センタ17に対してデータ名あるいはデータ番号を指定するとともに2次ユーザ情報Iu2を提示して2次利用申込を行うが、そのときに1次ユーザとの関係を明確にするために暗号化データCmks2に付加されている暗号化されていない1次ユーザ情報Iu1も提示する。著作権管理センタ17は、提示された1次ユーザ情報Iu1に基づきその1次ユーザがそのデータを2次利用するために第2秘密鍵Ks2の再交付を受けていることを確認し、復号化鍵である第2秘密鍵Ks2、暗号化／復号化鍵である第3秘密鍵Ks3を通信ネットワーク2を経由して2次ユーザ端末装置5に転送する。第2秘密鍵Ks2、第3秘密鍵Ks3を受け取った2次ユーザ端末装置5において、著作権管理プログラムPにより第2秘

密鍵Ks2を用いて暗号化データCmks2が復号化され
M= D（Ks2, Cmks2）
表示あるいは加工の2次利用が行われる。

【0076】このシステムにおいては、1次利用申込は鍵管理センタ16が処理し、2次利用申込は著作権管理センタ17が処理する。また、1次ユーザが供給されるデータMは第1秘密鍵Ks1を用いて暗号化されているが、2次ユーザが供給されるデータMは第2秘密鍵Ks2を用いて暗号化されている。一方、1次ユーザに対して鍵管理センタ16からは暗号鍵として第1秘密鍵Ks1及び第2秘密鍵Ks2が転送される。そのため、2次ユーザが1次ユーザであると偽って鍵管理センタ16に対して1次利用申込を行った場合には復号化鍵として第1秘密鍵Ks1が、暗号化／復号化鍵として第2秘密鍵Ks2が転送される。しかし、復号化鍵として転送された第1秘密鍵Ks1を用いて暗号化データCmks2を復号することはできない。したがって、データの利用について虚偽の申込を行うことは不可能であり、その結果データの原著作権だけでなく、データについての1次ユーザの著作権も保護される。

【0077】2次ユーザ端末装置5においてデータMの表示及び加工のための表示以外の利用形態である保存、コピー、転送が行われるときには著作権管理プログラムPによって第3秘密鍵Ks3を用いてデータMの暗号化が行われ、以後第3秘密鍵Ks3を用いてデータの復号及び暗号化が行われる。
Cmks3= E（Ks3, M）
M= D（Ks3, Cmks3）
なお、2次ユーザが表示及び加工を行い加工データM2を得ることも原則として自由にできるが、その場合は著作権管理プログラムPによってその回数に制限を設けることができる。

【0078】外部記憶媒体12にデータMがコピーされたとき及び通信ネットワーク2を経てデータが転送されたときには2次ユーザ端末装置5内の第2秘密鍵Ks2及び第3秘密鍵Ks3は著作権管理プログラムPによって廃棄される。したがって、2次ユーザが再度データMを利用する場合には著作権管理センタ3に利用申込を行い、第3秘密鍵Ks3の再交付を受ける必要がある。この第3秘密鍵Ks3の再交付を受けたことは、データMが外部記憶媒体12へコピーあるいは通信ネットワーク2を経由しての3次ユーザ端末装置6へ転送されることによる2次利用が行われたことを意味するから、このことが著作権管理センタ17に登録され、以後の利用が可能になる。

【0079】2次ユーザ端末装置5からの3次ユーザ端末装置6へのデータMの移動は外部記憶媒体12によってあるいは通信ネットワーク2により行われ、外部記憶媒体12へのコピーあるいは通信ネットワーク2を経由して移動が行われるときには、第3秘密鍵Ks3を用いてデータMが暗号化される。

【0080】外部記憶媒体12にデータMがコピーされたとき及び通信ネットワーク2を経てデータMが3次ユーザ端末装置6に転送されたときに2次ユーザ端末装置5内の第2秘密鍵Ks2及び第3秘密鍵Ks3は廃棄されるが、そのときに2次ユーザ端末装置5内に保存されている暗号化データCmks3に、暗号化されていない2次ユーザ情報Iu2が付加される、暗号化データCmks3を3次ユーザに転送する際に2次ユーザ情報Iu2も転送される。この各ユーザ情報のデータへの付加には、全てのユーザ情報がコピーあるいは転送の度にデータに付加される場合と、その度に最新のものに書き換えられる履歴が著作権管理センタに保管される場合がある。

【0081】2次ユーザからコピーあるいは転送された暗号化データCmks3の3次利用を希望する3次ユーザは、3次ユーザ端末装置6を利用して通信ネットワーク2を経由して著作権管理センタ17に対してデータ名あるいはデータ番号を指定するとともに3次ユーザ情報Iu3を提示して3次利用申込を行うが、そのときに2次ユーザとの関係を明確にするために暗号化データCmks3に付加されている暗号化されていない2次ユーザ情報Iu2も提示する。著作権管理センタ17は、提示された2次ユーザ情報Iu2に基づきその2次ユーザがそのデータを3次利用するための準備手続き、すなわち第3秘密鍵Ks3の再交付を受けていることを確認し、復号化鍵である第3秘密鍵Ks3、暗号化／復号化鍵である第4秘密鍵Ks4を通信ネットワーク2を経由して3次ユーザ端末装置6に転送する。第3秘密鍵Ks3、第4秘密鍵Ks4を受け取った3次ユーザ端末装置6において、著作権管理プログラムPにより第3秘密鍵Ks3を用いて暗号化データCmks3が復号化され
M= D（Ks3, Cmks3）
表示あるいは加工の3次利用が行われる。

【0082】このシステムにおいては、1次ユーザが供給されるデータMは第1秘密鍵Ks1を用いて暗号化され、2次ユーザが供給されるデータMは第2秘密鍵Ks2を用いて暗号化されているが、3次ユーザが供給されるデータMは第3秘密鍵Ks3を用いて暗号化されている。そのため、3次ユーザが1次ユーザであると偽って鍵管理センタ16に対して1次利用申込を行った場合には復号化鍵として第1秘密鍵Ks1が、暗号化／復号化鍵として第2秘密鍵Ks2が転送される。しかし、復号化鍵として転送された第1秘密鍵Ks1を用いて暗号化データCmks3を復号化することはできない。また、3次ユーザが2次ユーザであると偽って著作権管理センタ17に対して2次利用申込を行った場合には復号化鍵として第2秘密鍵Ks2が、暗号化／復号化鍵として第3秘密鍵Ks3が転送される。しかし、復号化鍵として転送された第2秘密鍵Ks2を用いて暗号化データCmks3を復号することはできない。したがって、データの利用について虚偽の申込

を行うことは不可能であり、その結果データの原著作権だけでなく、データについての1次ユーザの著作権及び2次ユーザの著作権も保護される。以下、同様の手続きが4次以降の利用にも適用される。

【0083】以上説明したシステムにおけるデータベース1、鍵管理センタ16、著作権管理センタ17は別個に設置されているが、これらは必ずしも別個のものである必要はなく、これらの全てあるいは適当な2つを一体に設置することも可能である。また、1次ユーザからの第2秘密鍵再交付申込は鍵管理センタ16に対して行うのではなく著作権管理センタ17に対して行うようにしてもよい。□

【0084】図7に示されたのは、デジタルビデオあるいはデジタルオーディオ等におけるデータの加工方法における信号処理フローであり、（a）に示されたのは、一般的に行われている加工フロー、（b）に示されたのは、信号の劣化を避けることができる加工処理フローである。（a）に示された加工フローにおいて、デジタル信号（61）として供給された信号は初めにアナログ化（62）され、次いでアナログ化された信号に対して表示64を行いながら加工（63）が行われ、加工が終了したアナログ信号は再デジタル化（65）されて保存，複写，転送（66）される。この過程は簡略ではあるが、信号の加工がアナログ状態で行われ、加工終了後再びデジタル化されるため、信号の劣化を避けることができない。

【0085】（b）に示された加工フローにおいて、デジタル信号（61）は加工のためにアナログ化（62）されて表示される。アナログ化（62）された信号は加工（63）において使用されるが、このアナログ化された信号は表示（64）に用いられるのみであって、保存，複写，転送には用いられない。保存，複写，転写用の信号は、アナログ化されて表示されている信号と対応してデジタル信号（61）の状態で、加工（67）され、保存，複写，転送（66）が行われる。この加工フローの場合には、保存，複写，転送されるデジタル信号がアナログ化されることはないから劣化は生じない。

【0086】図8に示されたのは、図6に示されたデジタルビデオあるいはデジタルオーディオ等におけるデータの加工方法における信号処理を暗号化されたデータを加工する場合に応用したフローの例であり、（a）に示されたのは、簡略化された信号処理フロー、（b）に示されたのは、著作権の管理を十分に行うことができる信号処理フローの例である。（a）に示された信号処理フローにおいて第1秘密鍵Ks1を用いて暗号化されて供給された原データCm0ks1 71は初めに第1秘密鍵Ks1を用いて復号化72され、

M0 ＝D（Ks1，Cm0ks1）

次いで復号化されたデータM0に対して表示（74）を行いながら加工（73）が行われる。加工が終了したデータM1は第2秘密鍵Ks2を用いて再暗号化（75）されて

Cm1ks2 ＝E（Ks2，M1）

保存，複写，転送（76）が行われる。この過程は簡略ではあるが、データの加工が復号化された状態で行われるため、復号化されたデータが保存，複写，転送されるおそれがあり、著作権の管理が十分に行われるとはいえない。

【0087】これに対して、（b）に示された信号処理フローにおいて、第1秘密鍵Ks1を用いて暗号化された原データCm0ks1（71）は第1秘密鍵Ks1を用いて復号化（72）され、

M0 ＝D（Ks1，Cm0ks1）

復号化されたデータM0が表示（74）される。一方、加工（73）は復号化データM0を手がかりにして暗号化データCm0ks1に対して行われ、保存用の原データM0あるいは加工された加工データM1は第2秘密鍵を用いて再暗号化され

Cm0ks2 ＝E（Ks2，M0）

Cm1ks2 ＝E（Ks2，M1）

暗号化データCm0ks2あるいはCm1ks2が保存，複写，転送（76）が行われる。復号化され表示されているデータと対応して復号化されることなく暗号化された状態で加工（77）され、その加工プログラムデータと暗号化されたままのデータが、保存，複写，転送（76）に用いられる。この信号処理フローの場合には、保存，複写，転送用のデータは暗号化されたままであるから、復号化されたデータが保存，複写，転送されることはない。

【0088】本願発明のデータ著作権管理装置が使用されるデータ著作権管理システムにおいては、入手した暗号化データを表示・加工する場合には復号化して利用するが、入手あるいは加工したデータを保存・複写・転送する場合には再暗号化することによって、データ著作権の管理を行う。しかし、図2に示された先願発明のデータ著作権管理装置15及び図3に記載された本発明のデータ著作権管理装置30は暗号化データの復号化あるいは復号化データの暗号化のいずれか一方しか行うことができない。そのため、復号化あるいは加工されたデータを保存・複写・転送する場合には一旦ユーザ端末装置あるいはデータ著作権管理装置のRAMに蓄積しておき、その後蓄積されたデータを再暗号化する必要がある。したがって、処理することができるデータに量的な制限が発生するばかりでなく、事故あるいは操作ミス等により復号化あるいは加工されたデータが失われるおそれがある。

【0089】一部の高級なMPUを除き、パーソナルコンピュータ等で使用される一般的なMPUは複数のマイクロコンピュータを同時に動作させるマルチプロセッサ構成について考慮されていない。したがって、パーソナ

ルコンピュータのシステムバスに付属装置を接続しても複数の作業を同時に行うことはできない。したがって、図2に示されたデータ著作権管理装置15あるいは図3に示されたデータ著作権管理装置30をユーザ端末装置20のシステムバス22に接続してもMPU21あるいは46とCPU16が並列して動作させることが可能なマルチプロセッサ構成とはならず、暗号化されたデータの復号化及び復号化されたデータの再暗号化の作業は同時に行われるのではなく、交互に行われる。そのため、復号化及び暗号化を行うことができるデータの大きさはRAMの容量に制限され、大きなデータを処理することはできない。また、大きなデータではない場合でも、処理速度を高くすることができない。

【0090】一方、先願発明として説明したデータ著作権管理システムにおいては、入手した暗号化データを表示・加工する場合には復号化して利用するが、入手あるいは加工したデータを保存・複写・転送する場合には再暗号化することによって、データの不正規な使用ができないようにしている。したがって、本発明が対象とするデータ著作権管理システムで使用される装置においては、データの復号化だけでなく、データの再暗号化も同時に行われることが望ましい。

【0091】一般的なパーソナルコンピュータにおいてマルチプロセッサ構成を実現する手段として、最近注目されているものにPCI（Peripheral Component Interconnect）バスがある。このPCIバスは、コンピュータのシステムバスにPCIブリッジを介して接続される外部接続用のバスであり、PCIバスを使用することでマルチプロセッサ構成を実現することができる。

【0092】図9に示されたのは、本発明実施例2である、PCIバスを使用するデータ著作権管理装置の構成であり、図3に示されたデータ著作権管理装置15と同じ構成すなわち、CPU16、CPU16のローカルバス17、ローカルバス17に接続されたROM18、RAM19及びEEPROM31を有するコンピュータシステムの構成を有している。一方、ユーザ端末装置20のマイクロプロセッサ21のシステムバス22にはPCIブリッジ82によって接続されるPCIバス81が接続されており、データ著作権管理装置80のCPU16のローカルバス17がこのPCIバス81に接続されている。ユーザ端末装置20のシステムバス22にはさらに、装置外部のデータベースからデータを受け取り、データを外部へ転送する通信装置（COMM）23、CD－ROMで供給されるデータを読み込むCD－ROMドライブ（CDRD）24、受け取ったデータあるいは加工したデータを外部へ供給するためにフレキシブルディスクドライブに複写するフレキシブルディスクドライブ（FDD）25及びデータを保存するハードディスクドライブ（HDD）26が接続される。なお、COMM23、CDRD24、FDD25及びHDD26はPCIバス81に接続することも可能である。また、ユーザ端末装置のシステムバス22には当然のこととしてROM、RAM等が接続されているが、この図においては記載が省略されている。

【0093】その他の部分の構成及び動作は図3に示された実施例1の場合と同様なのでここでは説明は省略する。復号化及び再暗号化の作業はユーザ端末装置20のMPU21とデータ著作権管理装置80のCPU16が分担して、一方が復号化を他方が再暗号化を同時に行う。この実施例におけるMPU21とCPU16はPCIバスによる並列動作を行うマルチプロセッサ構成であるため、高い処理速度を得ることができる。

【0094】ところで、パーソナルコンピュータ本体に外部装置を取り付けて使用するための代表的な手段として、この他にハードディスク装置あるいはCD－ROMドライブ等の外部記憶装置が接続されるSCSI（Small Computer System Interface）インターフェースがある。このSCSIインターフェースには、SCSIインターフェースが接続されるパーソナルコンピュータ本体も含めて最大8台の装置を接続することができ、8台の装置として複数のコンピュータを使用することができる。これら複数のコンピュータはどれも同等の役割を果たすことができ、言い換えれば、SCSIインターフェースは単なるインターフェースではなくマルチプロセッサバスとしての機能も有している。実施例3はこのSCSIインターフェースのマルチプロセッサバスとしての機能に着目し、実施例2のPCIバス81に代えてSCSIインターフェース86（以下、理解の便のため「SCSIインターフェース」を「SCSIバス」という。）を介してデータ著作権管理装置85をユーザ端末装置20のシステムバス22に接続する。

【0095】図10に示されたのは、SCSIバスを用いた本発明実施例3のデータ著作権管理装置の構成ブロック図である。この実施例3のデータ著作権管理装置85は、図3に示されたデータ著作権管理装置と同じ構成すなわち、CPU16、CPU16のローカルバス17、ローカルバス17に接続されたROM18、RAM19及びEEPROM31を有するコンピュータシステムの構成を有している。

【0096】一方、ユーザ端末装置20のマイクロプロセッサ21のシステムバス22にはSCSIコントローラ（SCSICONT）87によって制御されるSCSIバス86が接続されており、データ著作権管理装置85のCPU16のローカルバス17がこのSCSIバス86に接続されている。また、ユーザ端末装置20のシステムバス22にはさらに、装置外部のデータベースからデータを受け取り、データを外部へ転送する通信装置（COMM）23、CD－ROMで供給されるデータを読み込むCD－ROMドライブ（CDRD）24、受け取ったデータあるいは加工したデータを外部へ供給する

ためにフレキシブルディスクドライブに複写するフレキシブルディスクドライブ（ＦＤＤ）２５及びデータを保存するハードディスクドライブ（ＨＤＤ）２６が接続される。なお、ＣＯＭＭ２３、ＣＤＲＤ２４、ＦＤＤ２５及びＨＤＤ２６はＳＣＳＩバス８６に接続することも可能である。また、ユーザ端末装置のシステムバス２２には当然のこととしてＲＯＭ、ＲＡＭ等が接続されているが、この図においては記載が省略されている。

【００９７】その他の部分の構成及び動作は図３に示された実施例１の場合と同様なのでさらなる説明は省略する。復号化及び再暗号化の作業はユーザ端末装置２０本体のＭＰＵ２１とデータ著作権管理装置８５のＣＰＵ１６が分担して、一方が復号化を他方が再暗号化を同時に行い、ＭＰＵ２１とＣＰＵ１６はＳＣＳＩバス８６による並列動作を行うマルチプロセッサ構成であるため、高い処理速度を得ることができる。

【００９８】なお、この他にマルチプロセッサ構成を実現するための手段としてＳＣＩ（Scalable Coherent Interface）等も利用可能であり、さらに可能ならばバスを介することなくマイクロプロセッサ同士を接続してもよい。

【００９９】本願発明のデータ著作権管理装置が管理しようとするデータには、文字データの他にグラフィックデータ、コンピュータプログラム、デジタル音声データ、ＪＰＥＧ等の方式による静止画データ、さらにはＭＰＥＧ等による動画データがある。これまでに説明した実施例２のデータ著作権管理装置８０あるいは実施例３のデータ著作権管理装置８５はＰＣＩバスあるいはＳＣＳＩバスによってユーザ端末装置２０のマイクロプロセッサ２１のシステムバス２２に接続されることによりマルチプロセッサを構成している。このようなマルチプロセッサ構成の場合、ユーザ端末装置２０のＭＰＵ２１はシステム全体を制御する役割も果たす必要がある。データが文字データ、グラフィックスデータ等比較的低速・小容量のデータである場合にはＭＰＵ２１とＣＰＵ１６によるマルチプロセッサ構成でも復号化及び再暗号化によるデータ著作権管理は可能であるが、データがＪＰＥＧ静止画による動画、ＭＰＥＧ１あるいはＭＰＥＧ２による動画である場合には、データが高速・大容量であるためこのような構成によるデータ著作権管理は著しく困難である。

【０１００】図１１に示された第４実施例においては、このような事態に対処するためにＰＣＩバス８１に第１のデータ著作権管理装置８０及び第２のデータ著作権管理装置９０を接続することにより、マルチプロセッサシステムを構成している。第２のデータ著作権管理装置９０は第１のデータ著作権管理装置８０と同じ構成すなわち、ＣＰＵ９１、ＣＰＵ９１のローカルバス９４、ローカルバス９４に接続されたＲＯＭ９２、ＲＡＭ９３及びＥＥＰＲＯＭ９５を有している。なお、この実施例において第１のデータ著作権管理装置８０は暗号化されたデータの復号化を行い、第２のデータ著作権管理装置９０は復号化されたデータの再暗号化を行う。

【０１０１】暗号化されたデータの復号化を行う第１のデータ著作権管理装置８０のＲＯＭ１８には、データベースを利用するためのソフトウェア及びユーザデータ等の固定した情報が格納される。ＲＡＭ１９には鍵管理センタあるいは著作権管理センタから供給される復号化用の第１暗号鍵及びデータ著作権管理システムプログラムが格納される。同様に復号化されたデータの再暗号化を行う第２のデータ著作権管理装置９０のＲＯＭ９２には、データベースを利用するためのソフトウェア及びユーザデータ等の固定した情報が格納され、ＲＡＭ９３には鍵管理センタあるいは著作権管理センタから供給される再暗号化用の第２暗号鍵及びデータ著作権管理システムプログラムが格納される。なお、このマルチプロセッサ構成にはＳＣＳＩあるいはＳＣＩ等も利用可能であり、さらに可能ならばバスを介することなくマイクロプロセッサ同士を接続してもよい。

【０１０２】図２に示された先願発明及び図３を用いて説明した本発明の実施例１において、暗号化されたデータが供給される通信装置（ＣＯＭＭ）２３及びＣＤ－ＲＯＭドライブ（ＣＤＲＤ）２４はユーザ端末装置２０のシステムバスに接続されている。そのため、暗号化されたデータを復号化するためには、暗号化されたデータをユーザ端末装置２０のシステムバスとデータ著作権管理装置のローカルバスを経由させなければならず、処理速度の低下を招くおそれがある。これは、これらの付属装置をＰＣＩバスあるいはＳＣＳＩバスに接続した場合でも同様である。図１２に示された実施例５においては、処理速度の低下を防止するために暗号化されたデータが供給される通信装置２３及びＣＤ－ＲＯＭドライブ２４は復号化用データ著作権管理装置９７のローカルバス１７に接続される。

【０１０３】図１２に示された実施例５のデータ著作権管理装置９７は復号化用のデータ著作権管理装置であり、図３に示された実施例１のデータ著作権管理装置３０と基本的には同じ構成すなわち、ＣＰＵ１６、ＣＰＵ１６のローカルバス１７、ローカルバス１７に接続されたＲＯＭ１８、ＲＡＭ１９及びＥＥＰＲＯＭ３１を有するコンピュータシステムとして構成され、通信装置ＣＯＭＭ２３及びＣＤ－ＲＯＭドライブＣＤＲＤ２４はローカルバス１７に接続される。ＲＯＭ１８には、著作権管理プログラム、暗号アルゴリズムに基づく暗号プログラム及びユーザデータ等の固定した情報が格納されている。ＥＥＰＲＯＭ３１には著作権情報が格納される。なお、著作権管理プログラム及び暗号プログラムがデータベース等外部から供給される場合には、これらはＲＯＭ１８ではなく、ＥＥＰＲＯＭ３１に格納される。ＲＡＭ１９には鍵管理センタあるいは著作権管理センタから供

給される復号化用暗号鍵及びデータ著作権管理システムプログラムが格納される。COMM23あるいはCDRD24から供給された暗号化データはデータ著作権管理装置97で復号化され、ユーザ端末装置95に転送される。

【0104】以上説明した実施例4のデータ著作権管理装置80及び90は別体に構成されたものとして記載されているが、これらを一体に構成することが可能であることは言うまでもないことである。

【0105】実施例5のデータ著作権管理装置100をさらに発展させた実施例6のデータ著作権管理装置を図13に示す。図2に示された先願発明及び図3を用いて説明した本発明の実施例1において、再暗号化されたデータを保存するHDD26等の保存装置はユーザ端末装置20のシステムバス22に接続されている。したがって、再暗号化されたデータを保存するためには、ユーザ端末装置20のシステムバス22とデータ著作権管理装置15あるいはデータ著作権管理装置30のローカルバス17を経由させなければならず、処理速度の低下を招くおそれがある。これはこれらの付属装置をPCIバスあるいはSCSIバスに接続した場合でも同様である。図13に示された実施例6のデータ著作権管理装置100においては、図12に示された実施例5の通信装置COMM23及びCD－ROMドライブCDRD24がローカルバス17に接続された復号化用データ著作権管理装置97に加えて再暗号化されたデータを保存するHDD26等の保存装置を再暗号化用データ著作権管理装置101のローカルバス94に接続する。

【0106】この実施例6に示された再暗号化用のデータ著作権管理装置101は、図3に示されたデータ著作権管理装置30と基本的には同じ構成すなわち、CPU91、CPU91のローカルバス94、ローカルバス94に接続されたROM92、RAM93及びEEPROM95を有するコンピュータシステムとして構成され、ローカルバス94にHDD26が接続される。

【0107】ROM92には、著作権管理プログラム、暗号アルゴリズムに基ずく暗号プログラム及びユーザデータ等の固定した情報が格納されている。EEPROM95には著作権情報が格納される。なお、著作権管理プログラム及び暗号プログラムがデータベース等外部から供給される場合には、これらはROM92ではなく、EEPROM95に格納される。RAM93には鍵管理センタあるいは著作権管理センタから供給される再暗号化用暗号鍵及びデータ著作権管理システムプログラムが格納される。再暗号化用の著作権管理装置101で再暗号化されたデータはHDD26に保存される。

【0108】以上説明した実施例6のデータ著作権管理装置100及び101は別体に構成されたものとして記載されているが、これらを一体に構成することが可能であることは言うまでもないことである。

【0109】デジタルデータには、文字データの他にグラフィックデータ、コンピュータプログラム、デジタル音声データ、JPEG等の方式による静止画データ、さらにはMPEG等による動画データがある。データ著作物を利用するユーザ端末装置として代表的なものはパーソナルコンピュータ等のコンピュータ装置であるが、この他にテレビジョン受像器等の受信装置、これらの受信装置に付属して使用されるセットトップボックス、デジタル信号を保存するデジタルビデオテープレコーダ、デジタルビデオディスクレコーダ、デジタルオーディオテープ（DAT）等のデジタル記録装置あるいは携帯型端末装置（Personal Digital Assistants＝PDA）がある。

【0110】拡張ボード、ICカードあるいはPCカードとして構成された先願である特願平6－237673号に記載された図2のデータ著作権管理装置または図6のデータ著作権管理装置をコンピュータ装置、受信装置、セットトップボックス、デジタル記録装置あるいは携帯型端末装置であるユーザ端末装置に付加して使用することも可能であるが、付加時の手間及び障害の発生を考慮するとデータ著作権管理装置はユーザ端末装置に内蔵されていることが望ましい。

【0111】そのためには、本発明の各実施例においてはデータ著作権管理装置の形態としてモノリシックIC、ハイブリッドICあるいは内蔵サブボードの形態を採用して、パーソナルコンピュータ等のコンピュータ装置、テレビジョン受像器等の受信装置、これらの受信装置に付属して使用されるセットトップボックス、デジタル信号を保存するデジタルビデオテープレコーダ、デジタルビデオディスクレコーダ、デジタルオーディオテープ（DAT）等のデジタル記録装置あるいは携帯型端末装置（PDA）等のユーザ端末装置に内蔵させる。

【0112】さらに、以上説明したデータ著作権管理装置はデータの利用だけではなくディジタルキャッシュの流通及びテレビジョン会議システムに対しても適用可能である。これまでに種々提案されているディジタルキャッシュシステムは秘密鍵方式で暗号化ディジタルキャッシュデータを銀行預金口座あるいはクレジット会社のキャッシングサービスから転送してICカードに保存しており、入出力用の端末装置を利用して支払を行う。このICカードを電子財布として利用するディジタルキャッシュシステムは商店等入出力用の端末装置が設置されている場所であればどこでも使用可能である反面、入出力用の端末装置がない場所、例えば家庭等、では使用不可能である。

【0113】ところで、ディジタルキャッシュは暗号化データであるからICカード以外にも暗号化データを保存することができ、かつ支払先にデータを転送することができる装置であればどのようなものでもディジタルキャッシュデータを保存する電子財布として利用すること

ができる。具体的に電子財布として利用可能なユーザ端末装置としては、パーソナルコンピュータ、インテリジェントテレビジョン装置、携帯情報端末装置、ＰＨＳ(Personal Hadyphone System) 等ノ 携帯電話器、ｲﾝﾃﾘｼﾞｪﾝﾄ電話機、入出力機能を有するＰＣカード等がある。

【０１１４】このような端末装置をディジタルキャッシュ用の電子財布として利用することによる取引は、これまでに説明したデータ著作権管理システムの構成におけるデータベースを顧客側銀行に、1次ユーザ端末装置を顧客に、２次ユーザ端末装置を小売店に、著作権管理センタを小売店側銀行に、３次ユーザ端末装置を卸売またはメーカに置き換えることにより実現される。

【０１１５】ディジタルキャッシュを通信ネットワークを経由して転送することにより行われる取引システムの使用例を図１４を用いて説明する。この使用例は図１に示されたデータ著作権管理システムの構成を利用したものであり、この図において、１１１は顧客、１１２は顧客１１１の取引銀行、１１３は小売店、１１４は小売店１１３の取引銀行、１１５はメーカ、１１６はメーカ１１５の取引銀行、２は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡＴＶ回線等の通信ネットワークであり、顧客１１１、顧客の取引銀行１１２、小売店１１３、小売店の取引銀行１１４、メーカ１１５及びメーカの取引銀行１１６は通信ネットワーク２によって相互に接続可能とされている。このシステムにおいて、顧客１１１は銀行の他にキャッシングサービスを行うクレジット会社を利用することが可能であり、小売店とメーカとの間に適当な数の卸売り店を介在させることが可能である。また、１１７及び１１８はディジタルキャッシュデータが格納されるＩＣカードあるいはＰＣカードであり、通信ネットワークを利用しない場合に使用される。なお、この図において、破線で示されたのは暗号化されたディジタルキャッシュデータの経路であり、実線で示されたのは顧客，小売店あるいはメーカから銀行への要求の経路であり、１点鎖線で示されたのは各銀行からの秘密鍵の経路である。

【０１１６】この使用例では暗号鍵として顧客側銀行１１２が用意する第１秘密鍵及び顧客が生成する第２秘密鍵，小売店が生成する第３秘密鍵及びメーカが生成する第４秘密鍵が用いられる。この使用例では顧客側銀行１１２，小売り店側銀行１１４，メーカ側銀行１１６を別個のものとして説明するが、これらを一括して金融システムとして考えてもよい。

【０１１７】ディジタルキャッシュデータを暗号化／復号化するディジタルキャッシュ管理プログラムＰは顧客１１１に予め配布され、ユーザ端末装置に保存されている。また、ディジタルキャッシュ管理プログラムＰは銀行との取引が行われる毎にデータとともに転送されるようにすることもできる。さらに、ディジタルキャッシュ管理プログラムＰは全銀行において共通するものとすることが望ましい。顧客１１１はユーザ端末装置を利用して通信ネットワーク２を経由して金額を指定することにより、顧客側銀行１１２に預金口座からの預金の引出の申込を行うがこのときに顧客１１１の顧客情報Ｉｃを提示する。

【０１１８】顧客１１１から預金引出の申込を受けた顧客側銀行１１２は、第１秘密鍵Ｋs1を選択あるいは作成し、引出金額のディジタルキャッシュデータM0 をこの第１秘密鍵Ｋs1で暗号化し、

Ｃm0ks1=E（Ｋs1, M0）

暗号化ディジタルキャッシュデータＣm0ks1 及び復号鍵である第１秘密鍵Ｋs1を顧客１１１に転送するとともに、顧客情報Ｉｃ及び第１秘密鍵Ｋs1を保管する。この場合、第１秘密鍵Ｋs1は顧客側銀行１１２が予め用意したものから選択してもよいが、顧客が引き出し時に顧客情報Ｉｃを提示し、ディジタルキャッシュ管理プログラムＰにより、提示された顧客情報Ｉｃに基づいて作成することもできる。

Ｋs1= Ｐ（Ｉｃ）

このようにすれば、第１秘密鍵Ｋs1を顧客１１１に固有のものとすることができるばかりでなく、顧客１１１に対して第１秘密鍵Ｋs1を転送する必要がないため、システムの安全性が高くなる。また、第１秘密鍵Ｋs1は顧客側銀行１１２の銀行情報Ｉbsあるいは銀行情報Ｉbsと作成日時に基づいて作成することもできる。

【０１１９】暗号化ディジタルキャッシュデータＣm0ks1 及び第１秘密鍵Ｋs1を転送された顧客１１１は、ディジタルキャッシュ管理プログラムＰにより、顧客情報Ｉｃ，第１秘密鍵Ｋs1の何れか１つあるいは双方に基づいて第２秘密鍵Ｋs2を生成し、

Ｋs2= Ｐ（Ｉｃ）

生成された第２秘密鍵Ｋs2がユーザ端末装置内に保存される。また、顧客１１１はディジタルキャッシュ管理プログラムＰにより暗号化ディジタルキャッシュデータＣm0ks1 を第１秘密鍵Ｋs1を用いて復号化して

M0=D（Ｋs1, Ｃm0ks1）

内容を確認するが、内容が確認された復号化ディジタルキャッシュデータM0 が電子財布であるユーザ端末装置内に保存される場合には、生成された第２秘密鍵Ｋs2を用いてディジタルキャッシュ管理プログラムＰにより暗号化される。

Ｃm0ks2=E（Ｋs2, M0）

また、このときに第１秘密鍵Ｋs1が廃棄される。

【０１２０】小売店１１３から物品の購入を希望する顧客１１１は、ディジタルキャッシュ管理プログラムＰにより電子財布であるユーザ端末装置に保存されている暗号化ディジタルキャッシュデータＣm0ks2 を第２秘密鍵Ｋs2を用いて復号化し、

M0=D（Ｋs2, Ｃm0ks2）

必要な金額に対応するディジタルキャッシュデータM1

をディジタルキャッシュ管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化し、

Ｃm1ks2=E（Ks2，M1）

通信ネットワーク２を介して暗号化ディジタルキャッシュデータＣm1ks2 を小売店１１３の電子財布であるユーザ端末装置に転送することにより、支払を行う。そのときに、顧客情報Ｉｃも小売店１１３のユーザ端末装置に転送される。また、残額ディジタルキャッシュデータＭ２はディジタルキャッシュ管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化され、

Ｃm2ks2=E（Ks2，M2）

顧客１１１のユーザ端末装置内に保存される。

【０１２１】暗号化ディジタルキャッシュデータＣm1ks2 及び顧客情報Ｉｃを転送された小売店１１３は、転送された暗号化ディジタルキャッシュデータＣm1ks2 及び顧客情報Ｉｃをユーザ端末装置に保存するとともに、内容を確認するために通信ネットワーク２を経由して小売店側銀行１１４に顧客情報Ｉｃを提示して、復号鍵である第２秘密鍵Ｋs2の転送を依頼する。小売店１１３から第２秘密鍵Ｋs2の転送依頼を受けた小売店側銀行１１４は、第２秘密鍵Ｋs2の転送依頼とともに顧客情報Ｉｃを顧客側銀行１１２に転送する。小売店側銀行１１４から第２秘密鍵Ｋs2の転送依頼を転送された顧客側銀行１１２は、第２秘密鍵Ｋs2が顧客情報Ｉｃのみに基づいている場合にはディジタルキャッシュ管理プログラムＰにより顧客情報Ｉｃに基づいて第２秘密鍵Ｋs2を生成し、第２秘密鍵Ｋs2が顧客情報Ｉｃと第１秘密鍵Ｋs1に基づいている場合にはディジタルキャッシュ管理プログラムＰにより顧客情報Ｉｃと第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2を生成し、生成された第２秘密鍵Ｋs2を小売店側銀行１１４に転送する。顧客側銀行１１２から第２秘密鍵Ｋs2を転送された小売店側銀行１１４は、通信ネットワーク２を経由して第２秘密鍵Ｋs2を小売店１１３に転送する。

【０１２２】第２秘密鍵Ｋs2を転送された小売店１１３は、ディジタルキャッシュ管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化ディジタルキャッシュデータＣm1ks2 を復号化し、

M1=D（Ks2，Cm1ks2）

金額を確認の上、商品を顧客１１１に発送する。なお、この場合小売店１１１が小売店側銀行１１４ではなく顧客側銀行１１２に直接に第２秘密鍵Ｋs2の転送を依頼するようにすることもできる。

【０１２３】小売店１１３が収受したディジタルキャッシュを小売店側銀行１１４の口座に入金する場合には、通信ネットワーク２を経由して小売店側銀行１１４に暗号化ディジタルキャッシュデータＣm1ks2 とともに顧客情報Ｉｃを転送する。暗号化ディジタルキャッシュデータＣm1ks2 と顧客情報Ｉｃを転送された小売店側銀行１１４は、顧客情報Ｉｃを転送することにより第２秘密鍵Ｋs2の転送を顧客側銀行１１２に対して依頼する。小売店側銀行１１４から第２秘密鍵Ｋs2の転送を依頼された顧客側銀行１１２は、第２秘密鍵Ｋs2が顧客情報Ｉｃのみに基づいている場合にはディジタルキャッシュ管理プログラムＰにより顧客情報Ｉｃに基づいて第２秘密鍵Ｋs2を生成し、第２秘密鍵Ｋs2が顧客情報Ｉｃと第１秘密鍵Ｋs1に基づいている場合にはディジタルキャッシュ管理プログラムＰにより顧客情報Ｉｃと第１秘密鍵Ｋs1に基づいて第２秘密鍵Ｋs2を生成し、生成された第２秘密鍵Ｋs2を小売店側銀行１１４に転送する。顧客側銀行１１２から第２秘密鍵Ｋs2を転送された小売店側銀行１１４は、ディジタルキャッシュ管理プログラムＰにより第２秘密鍵Ｋs2を用いて暗号化ディジタルキャッシュデータＣm1ks2 を復号化し、

M1=D（Ks2，Cm1ks2）

復号化ディジタルキャッシュデータＭ1 を小売店１１４の銀行口座に入金する。

【０１２４】一般的な取引システムにおいては、小売店１１３はメーカ１１５あるいはメーカ１１５と小売店１１３の間に介在する卸売り店から商品を仕入れ、顧客１１１に販売する。そのため、顧客１１１と小売店１１３との間に存在するのと同様の取引形態が小売店１１３とメーカ１１５との間にも存在する。この小売店１１３とメーカ１１５との間で行われるディジタルキャッシュの取り扱いは、顧客１１１と小売店１１３との間で行われるディジタルキャッシュの取り扱いと基本的な相違はないため、煩雑さをさけるため説明を省略する。

【０１２５】このディジタルキャッシュシステムにおける、ディジタルキャッシュの取扱いはすべて銀行を介在させて行われるため、顧客側銀行にディジタルキャッシュの取扱いに関する金額，日付，秘密鍵要求者情報等の情報を保存しておくことにより、ディジタルキャッシュの残高及び使用履歴を把握することができる。また、ディジタルキャッシュデータを保存する電子財布であるユーザ端末装置が紛失あるいは破損により使用不能となった場合でも、顧客側銀行に保存されている使用残高及び使用履歴に基づきディジタルキャッシュを再発行することが可能である。なお、ディジタルキャッシュの安全性を高めるためにディジタルキャッシュデータにディジタル署名を付けることが望ましい。この使用例において、ディジタルキャッシュには顧客情報が付加されており、この顧客情報はディジタル署名付とされることがある。つまり、この実施例においてディジタルキャッシュは顧客を振り出し人とする手形決済システムとしての機能も有する。さらに、このシステムは従来紙を用いて行われている国際貿易における各種決済システム、例えば信用状（Letter of Credit:L/C）、（Bill of Lading:B/L),Payment of Settlement of Import/ Export にも拡張として応用することができる。

【０１２６】これまでは従来の音声電話器にテレビジョ

ン映像を付加したものに過ぎなかったテレビジョン会議システムが、最近はコンピュータシステムに組み込まれることにより音声あるいは映像の品質が向上したばかりでなく、コンピュータ上のデータも音声及び映像と同時に扱うことができるように進化している。このような中で、テレビジョン会議参加者以外の盗視聴による使用者のプライバシー侵害及びデータの漏洩に対するセキュリティーは秘密鍵を用いた暗号化システムによって保護されている。しかし、テレビジョン会議参加者自身が入手する会議内容は復号化されたものであるため、テレビジョン会議参加者自身が会議内容を保存し、場合によっては加工を行い、さらにはテレビジョン会議参加者以外の者に配布する２次的な利用が行われた場合には他のテレビジョン会議参加者のプライバシー及びデータのセキュリティーは全く無防備である。特に、伝送データの圧縮技術が発達する一方でデータ蓄積媒体の大容量化が進んだ結果テレビジョン会議の内容全てがデータ蓄積媒体に複写されたりあるいはネットワークを介して転送される恐れさえ現実のものとなりつつある。

【０１２７】この使用例はこのような状況に鑑みて、これまでに説明したデータ著作権管理システムの構成をテレビジョン会議システムに応用することにより、テレビジョン会議参加者自身の２次的な利用による他のテレビジョン会議参加者のプライバシー及びデータのセキュリティー確保を行うものである。

【０１２８】このテレビジョン会議データ管理システムは、例えば図１に示されたデータ著作権管理システムの構成におけるデータベースをテレビジョン会議第１参加者に、１次ユーザ端末装置をテレビジョン会議第２参加者に、２次ユーザ端末装置をテレビジョン会議非参加者に置き換えることにより実現することができる。この使用例を図１５を用いて説明する。この図において、１２１はテレビジョン会議第１参加者、１２２はテレビジョン会議第２参加者、１２３はテレビジョン会議第３非参加者、１２４はテレビジョン会議第４非参加者、２は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡテレビジョン回線等の通信ネットワークであり、テレビジョン会議第１参加者１２１とテレビジョン会議第２参加者１２２は通信ネットワーク２によって相互に接続可能とされている。また、テレビジョン会議第２参加者１２２とテレビジョン会議第３非参加者１２３、テレビジョン会議第３非参加者１２３とテレビジョン会議第４非参加者１２４は通信ネットワーク２で接続可能とされている。また、１２５及び１２６はデータ記録媒体である。この図において、破線で示されたのは暗号化されたテレビジョン会議内容の経路であり、実線で示されたのはテレビジョン会議第３非参加者１２３及びテレビジョン会議第４非参加者１２４からテレビジョン会議第１参加者１２１へ暗号鍵を要求する経路であり、１点鎖線で示されたのはテレビジョン会議第１参加者１２１からテレビジョン会議第２参加者１２２、テレビジョン会議第３非参加者１２３及びテレビジョン会議第４非参加者１２４へ暗号鍵が転送される経路である。なお、この使用例で説明するテレビジョン会議データ管理システムでは説明を簡明にするために、テレビジョン会議第１参加者１２１のデータベース及びデータセキュリティーの確保のみが行われる場合について説明するが、テレビジョン会議第２参加者１２２のプライバシー及びデータセキュリティーの確保も行うことが可能であることはいうまでもない。

【０１２９】映像及び音声を含むテレビジョン会議第１参加者１２１のテレビジョン会議データを暗号化／復号化するテレビジョン会議管理プログラムＰはテレビジョン会議第２参加者１２２、テレビジョン会議第３非参加者１２３及びテレビジョン会議第４非参加者１２４に予め配布され、各々の端末装置に内蔵されている。なお、テレビジョン会議データ管理プログラムＰは暗号鍵が転送される毎に転送されるようにすることもできる。さらに、この使用例では暗号鍵としてテレビジョン会議第１参加者１２１が用意する第１秘密鍵及びテレビジョン会議第２参加者１２２が生成する第２秘密鍵，テレビジョン会議第３非参加者１２３が生成する第３秘密鍵・・・が用いられる。

【０１３０】テレビジョン会議第１参加者１２１とテレビジョン会議第２参加者１２２は、各端末装置を利用し、通信ネットワーク２を経由して音声，映像，データ（これらを一括して「テレビジョン会議データ」と呼ぶ）を相互に転送することによりテレビジョン会議を行うが、テレビジョン会議を開始する前にテレビジョン会議第１参加者１２１は第１秘密鍵Ｋs1を選択あるいは生成し、第１秘密鍵Ｋs1をテレビジョン会議を開始する前にテレビジョン会議第２参加者１２２に供給する。また、第１秘密鍵Ｋs1を転送されたテレビジョン会議第２参加者１２２は、テレビジョン会議データ管理プログラムＰにより、第１秘密鍵Ｋs1基づいて第２秘密鍵Ｋs2を生成し、

$$K_{s2}= P\ (K_{s1})$$

生成された第２秘密鍵Ｋs2を端末装置内に保存しておく。

【０１３１】テレビジョン会議第１参加者１２１は、通信ネットワーク２を経由して行われるテレビジョン会議において、テレビジョン会議データＭ0 を第１秘密鍵Ｋs1で暗号化し、

$$C_{m0ks1}=E\ (K_{s1},\ M0\ )$$

暗号化されたテレビジョン会議データＣm0ks1 をテレビジョン会議第２参加者１２２に転送する。

【０１３２】第１秘密鍵Ｋs1を用いて暗号化されたテレビジョン会議データＣm0ks1 を受け取ったテレビジョン会議第２参加者１２２は、第１秘密鍵Ｋs1を用いて暗号化テレビジョン会議データＣm0ks1 を復号し、

M0=D（Ks1, Cm0ks1）
復号化されたテレビジョン会議データM0を利用する。また、テレビジョン会議データ管理プログラムPにより、第1秘密鍵Ks1に基づいて第2秘密鍵Ks2が生成される。
Ks2= P（Ks1）
【0133】復号されたテレビジョン会議データM0がテレビジョン会議第2参加者122の端末装置内に保存される場合、データ記録媒体125に複写される場合、通信ネットワーク2を経由してテレビジョン会議第3非参加者に転送される場合には、そのデータMはテレビジョン会議データ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。
Cmks2= E（Ks2, M）
【0134】暗号化データCmks2は、テレビジョン会議データ名あるいはテレビジョン会議データ番号とともに、記録媒体125に複写され、あるいは、通信ネットワーク2を経由してテレビジョン会議第3非参加者に供給される。
【0135】暗号化データCmks2を入手したテレビジョン会議第3非参加者123は端末装置を利用して、テレビジョン会議データ名あるいはテレビジョン会議データ番号を指定することによりテレビジョン会議データMの2次利用をテレビジョン会議第1参加者121に申し込む。
【0136】データMの2次利用申込を受けたテレビジョン会議第1参加者121は、テレビジョン会議データ名あるいはテレビジョン会議データ番号を手がかりとして第1秘密鍵Ks1を探し出し、第1秘密鍵Ks1に基づいて第2秘密鍵Ks2を生成し、Ks2= P（Ks1）生成された第2秘密鍵Ks2をテレビジョン会議第3非参加者123に供給する。
【0137】第2秘密鍵Ks2を受け取ったテレビジョン会議第3非参加者123は、暗号化データCmks2をテレビジョン会議データ管理プログラムPを利用して第2秘密鍵Ks2を用いて復号化して
M= D（Ks2, Cmks2）
復号化されたテレビジョン会議データMを利用する。テレビジョン会議データMがテレビジョン会議第3非参加者123の端末装置内に保存される場合、記録媒体126に複写される場合、通信ネットワーク2を経由してテレビジョン会議第4非参加者124に転送される場合には、そのテレビジョン会議データMはテレビジョン会議データ管理プログラムPにより第2秘密鍵Ks2を用いて暗号化される。
Cmks2= E（Ks2, M）
【0138】なお、さらにテレビジョン会議データ管理プログラムPにより第2秘密鍵Ks2に基づいて第3秘密鍵Ks3が生成され、
Ks3= P（Ks2）
テレビジョン会議データ管理プログラムPによりこの生成された第3秘密鍵Ks3を用いてデータMが暗号化されるようにすることもできる。
Cmks3= E（Ks3, M）
【図面の簡単な説明】
【図1】　先願発明のデータ著作権管理システムの構成図。
【図2】　先願発明のデータ著作権管理装置の構成図。
【図3】　本発明実施例1のデータ著作権管理装置の構成図。
【図4】　本発明実施例1のデータ著作権管理装置の具体的な構成図。
【図5】　本発明に係るデータ著作権管理システムの処理フロー図。
【図6】　先願発明のデータ著作権管理システムの構成図。
【図7】　ディジタルデータの一般的な加工処理フロー図。
【図8】　本発明による暗号化データの加工処理フロー図。
【図9】　本発明実施例2のデータ著作権管理装置の構成図。
【図10】　本発明実施例3のデータ著作権管理装置の構成図。
【図11】　本発明実施例4のデータ著作権管理装置の構成図。
【図12】　本発明実施例5のデータ著作権管理装置の構成図。
【図13】　本発明実施例6のデータ著作権管理装置の構成図。
【図14】　本発明の使用例であるディジタルキャッシュシステムの構成図。
【図15】　本発明の使用例であるテレビジョン会議システム構成図。
【符号の説明】
1　データベース
2　通信ネットワーク
3，10，17　著作権管理センタ
4，5，6，7　ユーザ端末装置
11，12，13　記録媒体
14　放送・通信衛星
15'　CD－ROM
16　鍵管理センタ
17，22　マイクロコンピュータバス
18　読み出し専用メモリ
19　書き込み・読み出しメモリ
20　ユーザ端末装置
21，16　マイクロコンピュータ
22　ユーザ端末装置のシステムバス
23　通信装置

37

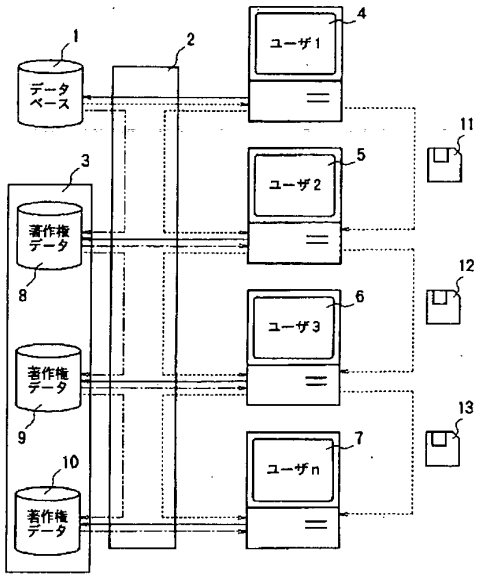
２４　ＣＤ－ＲＯＭドライブ
２５　フレキシブルディスクドライブ
２６　ハードディスクドライブ
３０，８０，８５，９０，９７，１００，１０１　データ著作権管理装置
３１　電気電気的消去可能プログラマブルメモリ
１１１　顧客
１１３　小売店

38

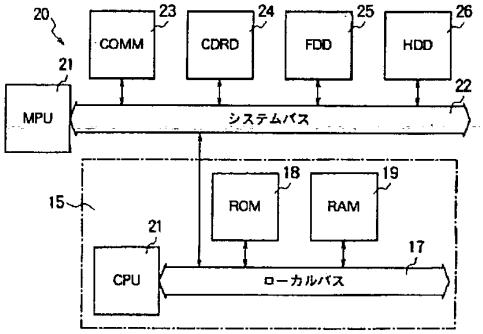
＊１１５　メーカ
１１２　顧客側銀行
１１４　小売店側銀行
１１６　メーカ側銀行
１１７，１１８　ＩＣカード
１２１，１２２　テレビジョン会議参加者
１２３，１２４　テレビジョン会議非参加者

＊

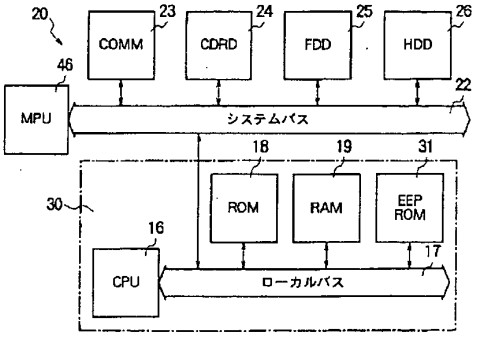
【図１】



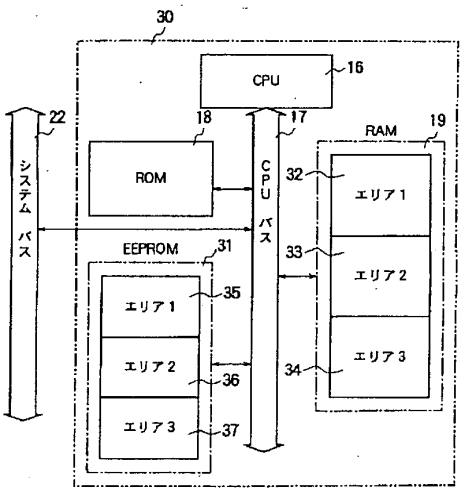
【図２】



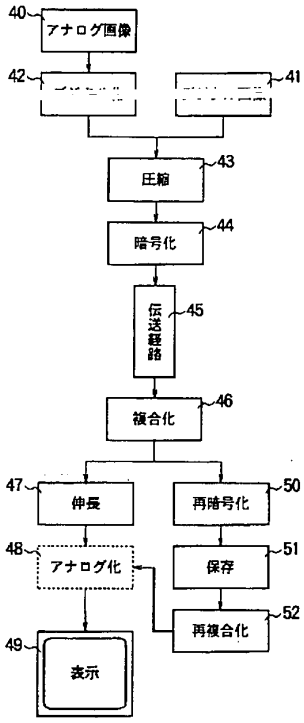
【図３】



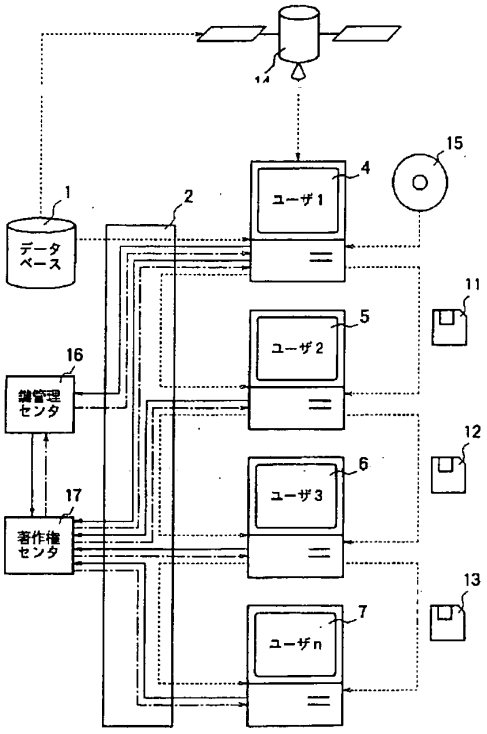
【図４】



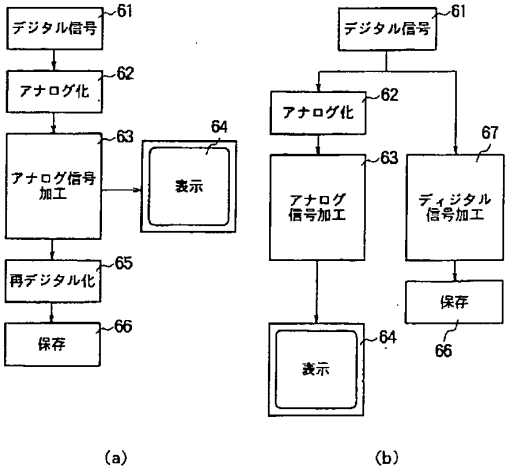
【図５】


40
アナログ画像
42
41
圧縮
43
暗号化
44
伝送経路
45
複合化
46
47
伸長
50
再暗号化
48
アナログ化
51
保存
52
再複合化
49
表示

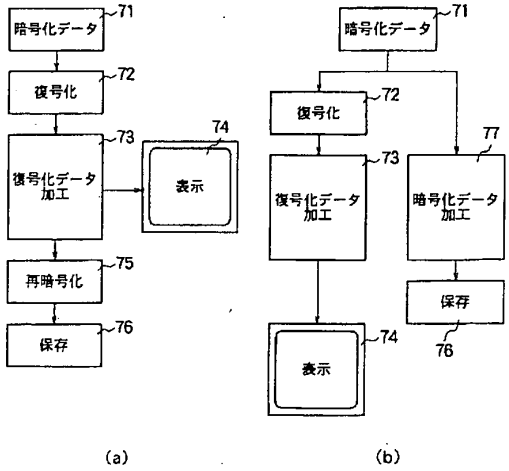
【図６】


14
15
1
データベース
2
ユーザ１
4
11
ユーザ２
5
16
鍵管理センタ
12
ユーザ３
6
17
著作権センタ
13
ユーザｎ
7

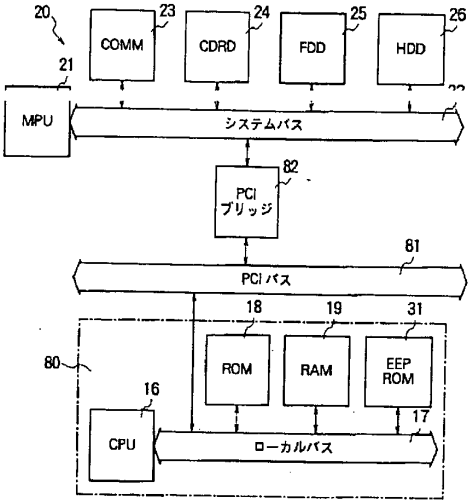
【図７】


デジタル信号
61
アナログ化
62
アナログ信号加工
63
64
表示
再デジタル化
65
保存
66
(a)
デジタル信号
61
アナログ化
62
67
アナログ信号加工
ディジタル信号加工
保存
66
表示
64
(b)

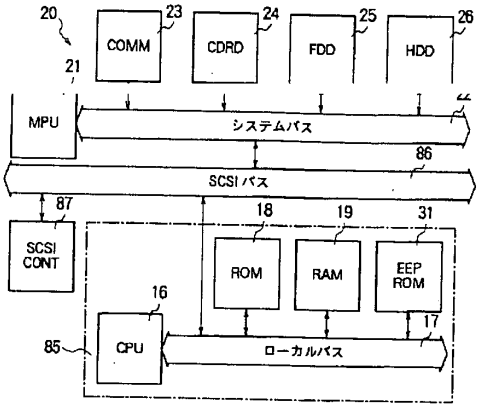
【図８】


暗号化データ
71
復号化
72
73
74
復号化データ加工
表示
再暗号化
75
保存
76
(a)
暗号化データ
71
復号化
72
77
復号化データ加工
暗号化データ加工
保存
76
表示
74
(b)

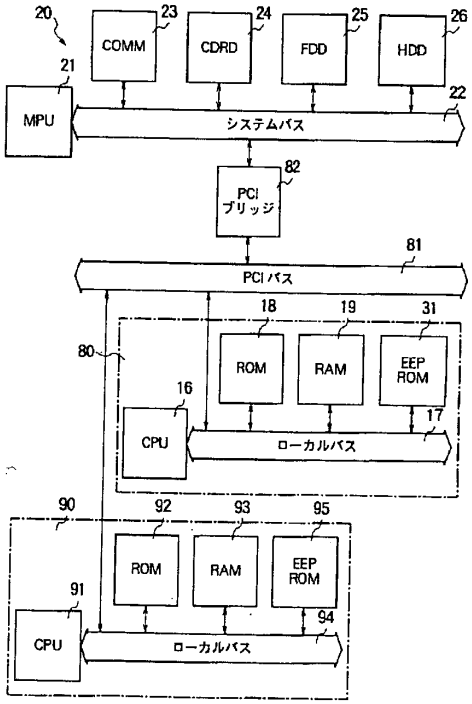
【図9】



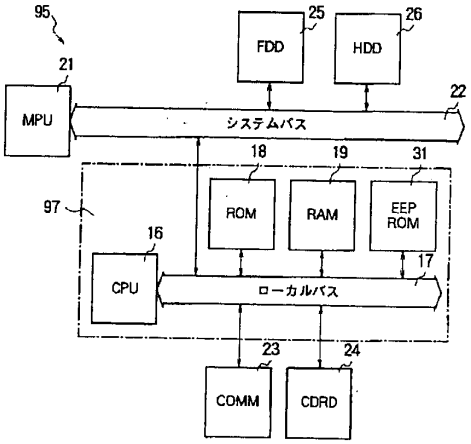
【図10】



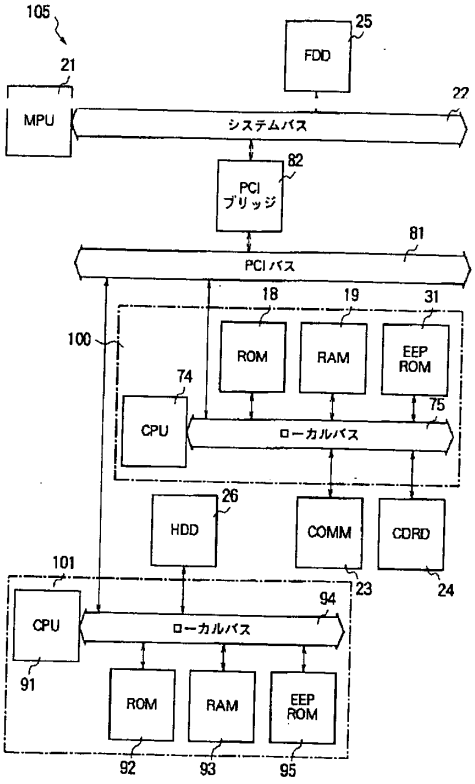
【図11】



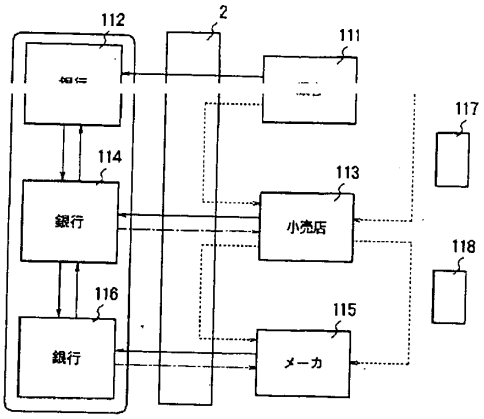
【図12】



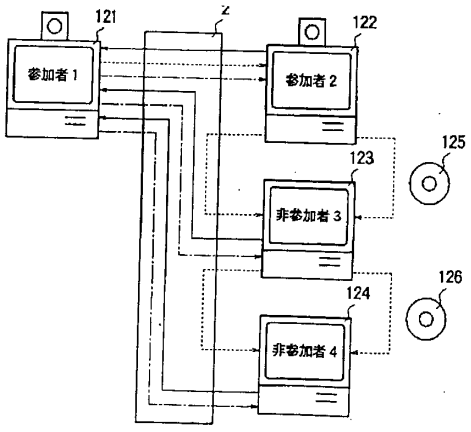
【図13】


105
21
MPU
25
FDD
22
システムバス
82
PCI
ブリッジ
81
PCIバス
18
19
31
100
ROM
RAM
EEP
ROM
74
CPU
75
ローカルバス
26
HDD
COMM
CDRD
101
23
24
94
CPU
ローカルバス
91
ROM
RAM
EEP
ROM
92
93
95

【図14】


112
2
111
117
114
銀行
113
小売店
118
116
銀行
115
メーカ

【図15】


121
参加者1
122
参加者2
125
123
非参加者3
126
124
非参加者4

フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
H04L	9/10		8842－5J	H04L	9/00	601F
	9/32		8842－5J			621A
H04N	7/15		8842－5J			627Z